

Referat privind necesitatea scoaterii la concurs a postului didactic de lector universitar 33 din cadrul Departamentului de Informatică

1. Necesitatea ocupării postului în contextul realizării obiectivelor din planul de dezvoltare al facultății

Strategia de dezvoltare pe termen mediu și lung a Facultății de Matematică și Informatică are ca obiective principale consolidarea echipei academice prin atragerea de tineri profesioniști cu o pregătire solidă și un potențial ridicat de performanță, precum și sprijinirea cadrelor didactice existente în atingerea obiectivelor lor de carieră. În prezent, **Departamentul de Informatică** este format din 39 de cadre didactice titulare (6 profesori, 10 conferențieri, 15 lectori, 7 asistenți universitari și 1 asistent de cercetare), deși statul de funcții include 89 de poziții. Această discrepanță se datorează creșterii numărului de studenți, în special la nivelul ciclului de licență, și scăderii interesului absolvenților de informatică pentru o carieră academică.

În aceste condiții, departamentul apelează anual la peste 40 de specialiști din industria IT pentru a susține cursuri de specialitate. Deși această colaborare este benefică prin expunerea studenților la realitățile din companiile IT, este necesară întărirea colectivului de cadre didactice propriu. Acest demers este esențial atât pentru îndeplinirea cerințelor specifice evaluărilor instituționale, cât și pentru asigurarea unui raport adecvat între numărul de cadre didactice și cel de studenți.

Consolidarea echipei academice presupune atât recrutarea tinerilor pe poziții de asistent universitar și lector, cât și atragerea unor specialiști cu experiență pentru pozițiile superioare. Pe lângă menținerea nivelului actual de înscrieri, există o cerere în creștere pe piața muncii pentru specialiști în informatică, în special în domeniile emergente precum inteligența artificială și prelucrarea datelor. Acest lucru subliniază necesitatea unei pregătiri riguroase la nivel universitar, iar angajarea unui cadru didactic pentru a acoperi disciplinele din planul de învățământ este o investiție directă în viitorul profesional al studenților.

2. Valoarea științifică ce se pretinde candidaților

Pentru înscrierea la concurs, candidații trebuie să îndeplinească condițiile stabilite prin Ordinul privind aprobarea standardelor minimale necesare și obligatorii pentru conferirea titlurilor didactice din Legea Învățământului Superior nr. 199/2023, cu modificările și completările ulterioare; în HG nr. 1339 din 29.12.2023 privind aprobarea Metodologiei-cadru de concurs pentru ocuparea posturilor didactice și de cercetare vacante din învățământul superior.

Toate concursurile se desfășoară în conformitate cu *Metodologia privind organizarea concursurilor de ocupare a posturilor didactice și de cercetare vacante din cadrul departamentelor academice ale UVT, a examenelor de promovare în cariera didactică din UVT și a examenelor de promovare în grade profesionale de cercetare-dezvoltare superioare a personalului de cercetare din cadrul departamentelor academice ale UVT*, intrată în vigoare prin Hotărârea Senatului UVT nr. 3 din 11.03.2024 (Modificarea 1 prin Hotărârea Senatului UVT nr. 19 din data de 26.09.2024; Modificarea 2 prin Hotărârea Senatului UVT nr. 27 din data de 20.02.2025), precum și standardele minimale pentru posturile didactice și de cercetare specifice domeniului Informatică din cadrul Facultății de Matematică și Informatică, Universitatea de Vest din Timișoara. Candidații trebuie să aibă activitate științifică reflectată prin rezultate publicate în ultimii doi ani în reviste de specialitate/ volume ale unor conferințe cu caracter internațional.

3. Perspectivele postului

Estimările actuale, bazate pe tendințele din ultimii ani privind numărul de studenți, sugerează că înscrierile la programele de studii în Informatică, Informatică în limba engleză și Inteligență Artificială, cu predare în limba engleză, vor rămâne cel puțin la nivelul actual. Prin urmare, poziția scoasă la concurs este justificată atât din perspectiva acoperirii necesare a disciplinelor din planurile de învățământ, cât și din punct de vedere financiar.

Postul include predarea unor discipline obligatorii în cadrul programelor de licență, cum ar fi *Proiect colectiv și Securitate și criptografie* pentru studenții de la Informatică, *Operating systems I* pentru cei de la Informatică și Inteligență Artificială cu predare în limba engleză, precum și *Cryptography and information security* pentru studenții de la masterul Cybersecurity. Aceste cursuri și laboratoare sunt importante pentru formarea specialiștilor în informatică, fiind parte din nucleul pregătirii acestora. Cursurile și laboratoarele menționate anterior au fost asociat unor posturi vacante, ceea ce indică faptul că aceste discipline vor continua să facă parte din planurile de învățământ ale specializărilor de licență din domeniul informaticii.

În contextul digitalizării și al creșterii volumului de date ce trebuie colectate, conectate și integrate, formarea specialiștilor capabili să proceseze și să gestioneze aceste date devine esențială.

4. Numărul posturilor existente deja în aceeași specialitate

În prezent, în statul de funcții al *Departamentului de Informatică* din cadrul *Facultății de Matematică și Informatică* se regăsesc 6 posturi de profesor (toate ocupate de titulari), 10 posturi de conferențiar (dintre care 10 sunt ocupate de titulari), 42 de posturi de lector (cu 15 posturi ocupate de titulari), 30 de posturi de asistent (dintre care doar 7 sunt ocupate de titulari) și un post de asistent de cercetare, care este, de asemenea, ocupat.

Printre disciplinele oferite de departament se numără *Proiect colectiv și Securitate și criptografie, Operating systems I și Cryptography and information security*, care sunt discipline

în planul de învățământ de la anul II, III de la specializările de Informatică cu predare în limba română sau engleză, dar și de la masterul de Cybersecurity. Până în prezent, aceste cursuri au fost susținute de cadre didactice asociate. Având în vedere importanța acestor discipline, considerăm că implicarea unor cadre didactice titulare în predarea lor ar aduce un beneficiu semnificativ. Titularii oferă o continuitate și o stabilitate mai mare în procesul educațional, asigurând o calitate superioară a predării și o mai bună integrare a cercetării în activitatea academică.

În plus, titularizarea unor cadre didactice ar contribui la întărirea echipei academice și la o mai bună coordonare a curriculumului. Acest lucru ar permite o mai bună adaptare a conținutului cursurilor la nevoile pieței muncii și la noile tehnologii, crescând astfel competitivitatea programelor de studiu. De asemenea, titularii ar putea să dezvolte noi direcții de cercetare și să se implice mai activ în formarea și mentoratul studenților, sporind calitatea actului educațional și contribuind la dezvoltarea unor competențe avansate la absolvenți.

5. Analiza statistică pe ultimii 3 ani privind evoluția numărului de candidați și de studenți înmatriculați la programele de studii unde se desfășoară activitățile din cadrul posturilor scoase la concurs sau pentru care se organizează examen de promovare în cariera didactică, după caz

Din datele existente la secretariatul Facultății de Matematică și Informatică, rezultă următoarea statistică cu privire la numărul de studenți înmatriculați în anul I la domeniul Informatică la nivelul de licență în ultimii 3 ani:

Programe de studii licență	2022-2023	2023-2024	2024-2025
Număr locuri scoase la concurs	350	425	425
Număr candidați	764	806	888
Număr studenți înmatriculați	328	359	355

Tendința crescătoare a numărului de candidați înscriși la examenul de admitere este justificată de interesul pentru domeniul Informatică. În ultimii doi ani universitari se observă o creștere a numărului de locuri scoase la concurs, implicit a numărului de studenți din anul I datorită înființării a două noi specializări Informatică ID și Inteligență Artificială cu predare în limba română.

Numărul studenților înmatriculați în anul I în ultimii 3 ani, la programele de master în domeniul Informatică este:

Program de studii master	2021-2022	2022-2023	2023-2024
Număr locuri scoase la concurs	200	200	200
Număr candidați	185	147	229
Număr studenți înmatriculați	182	143	198

În ultimul an universitar se observă creșterea numărului de studenți înmatriculați la programele de studii de masterat, ajungându-se anul acesta la capacitatea maximă de școlarizare.

6. Strategia de dezvoltare a resurselor umane, inclusiv situația pensionabililor în următorii 5 ani

Strategia de dezvoltare a resurselor umane în cadrul Facultății de Matematică și Informatică include următoarele acțiuni cheie:

- **Atragerea de specialiști de prestigiu**, inclusiv din industrie, cu recunoaștere științifică și profesională certificată.
- **Recrutarea absolvenților UVT** care au finalizat programe de doctorat sau postdoctorat în UVT, dar și în instituții de prestigiu internațional.
- **Promovarea cadrelor didactice** pe poziții superioare în concordanță cu nevoile academice și planurile lor de carieră.
- **Sprijinirea obținerii atestatului de abilitare** pentru cadrele didactice și cercetătorii care îndeplinesc standardele minimale CNATDCU.

Un obiectiv esențial al strategiei este ocuparea eficientă a posturilor didactice prevăzute în statul de funcții. În prezent, raportul dintre numărul de cadre didactice titulare și numărul de posturi este de **0.415**, semnificativ mai mic decât ținta optimă de **0.65-0.70**, necesară pentru o acoperire eficientă.

În următorii cinci ani, trei membrii ai departamentului vor ajunge la vârsta legală de pensionare, ceea ce face și mai necesară o bună acoperire a posturilor pentru a evita supraîncărcarea cadrelor didactice, care poate afecta negativ activitățile academice, în special cercetarea științifică.

Strategia urmărește menținerea unei **structuri piramidale echilibrate** în ierarhia didactică, promovarea treptată a cadrelor și evitarea promovărilor masive sau bruște. Un flux constant de promovări și cooptarea de noi specialiști este esențială pentru asigurarea calității academice. Scoaterea periodică la concurs a posturilor de la baza și vârful ierarhiei este un factor motivațional pentru cadrele didactice, stimulând creșterea performanței și atingerea unor standarde profesionale superioare.

7. Strategia cercetării științifice a departamentului/școlii doctorale și modul în care ocupantul postului ar trebui să se integreze acestei strategii

Strategia privind activitatea de cercetare din cadrul Departamentului de Informatică urmează direcțiile principale prevăzute în strategia de cercetare de la nivelul UVT și cea a Facultății de Matematică și Informatică având ca scop crearea unui mediu de cercetare performant și atractiv pentru specialiști, în particular pentru tinerii cercetători, promovarea excelenței în ceea ce privește rezultatele cercetării științifice și stimularea competitivității în atragerea de fonduri naționale și internaționale.

7.1 Organizarea activității de cercetare

Activitatea de cercetare în informatică se desfășoară în cadrul a două entități:

- Centrul de Cercetare în Informatică (CCI - <http://research.info.uvt.ro>) acreditată la nivel național. În cadrul acestui centru activează la ora actuală 7 grupuri de cercetare:

- Cloud Computing, HPC și IoT
- Aplicații și Analiză Big Data
- Inteligență Artificială și Machine Learning
- Signal, Image and Machine Learning
- Aplicații în Earth Observation
- Teoria Calculului
- Matematică Computațională și Aplicată
- Securitate Cibernetică

- Institutul e-Austria (<http://www.ieat.ro>) care este un spin-off de cercetare constituit în cadrul unui parteneriat dintre Universitatea de Vest, Universitatea Politehnica din Timișoara și Institutul RISC din Linz, Austria.

În cadrul acestor entități sunt derulate proiecte de cercetare naționale și internaționale.

7.2 Obiective strategice în activitatea de cercetare

Obiective generale la nivelul Facultății de Matematică și Informatică sunt:

- ❖ Intensificarea relațiilor de cooperare internațională și integrarea în rețele tematice de cercetare în domeniile matematicii și tehnologiei informației în corelație cu prioritățile Uniunii Europene;
- ❖ Dezvoltarea unor relații eficiente de parteneriat cu instituții naționale și internaționale;
- ❖ Stimularea activităților de creștere a vizibilității cercetării științifice din Facultatea de Matematică și Informatică prin valorificarea specifică a

rezultatelor în reviste de specialitate cu factor de impact ridicat și largă recunoaștere internațională;

- ❖ Ridicarea impactului internațional al publicațiilor proprii. Atragerea unor specialiști renumiți din străinătate ca membri în colectivul de redacție al Analelor Facultății de Matematică și Informatică, Universității de Vest, seria Matematică și Informatică, pentru creșterea exigenței evaluării lucrărilor publicate în aceste reviste;
- ❖ Valorificarea excelenței în cercetare prin participarea la competițiile de atribuire a noilor proiecte din cadrul programelor naționale și internaționale și prin implicare în creșterea performanțelor în activitățile din mediul socio-economic;
- ❖ Revitalizarea și revigorarea activității de cercetare științifică studentească prin integrarea în colectivele de cercetare a unor studenți, de la studiile de licență, master și doctorat;
- ❖ Sprijinirea doctoratelor în cotutelă;
- ❖ Atragerea de studenți străini la studiile doctorale;
- ❖ Dezvoltarea unor studii universitare de masterat în limbi străine și a programelor masterale în parteneriat cu institute de învățământ superior precum și reprezentanți din mediu socio-economic din țară și străinătate.

Obiective specifice activității de cercetare de la Departamentul de Informatică:

- ❖ consolidarea grupurilor de cercetare existente prin atragerea de tineri cercetători;
- ❖ identificarea unor noi direcții de cercetare, aliniate direcțiilor strategice urmate la nivel național și european și constituirea unor noi grupuri de cercetare prin:
 - facilitarea accesului la resurse de documentare;
 - invitarea unor cercetători din țară și străinătate pentru a susține prezentă în cadrul Seminarului științific al CCI.
- ❖ identificarea de teme de cercetare-dezvoltare aplicativă în parteneriat cu mediul privat prin:
 - organizarea de întâlniri între grupurile de cercetare și reprezentanți ai companiilor;
 - încurajarea cercetătorilor să aplice la apelurile naționale dedicate proiectelor de transfer tehnologic și a celor experimental demonstrative;
 - stimularea activității antreprenoriale a tinerilor cercetători și a studenților. stimularea colaborării cu alte centre de cercetare din cadrul Universității de Vest din Timișoara;
- ❖ creșterea vizibilității grupurilor de cercetare din cadrul CCI prin:
 - publicații în reviste de specialitate cu impact;
 - participarea la conferințe internaționale de top și alte evenimente care facilitează stabilirea de contacte între cercetători;

- participarea la elaborarea de propuneri de proiecte pentru competițiile lansate în cadrul programelor finanțate de Comisia Europeană;
- organizarea de manifestări științifice cu caracter internațional și creșterea nivelului de recunoaștere internațională conferinței SYNASC(<http://synasc.ro>);
- creșterea nivelului calitativ și promovarea revistei Scalable Computing: Practice and Experience (<http://www.scpe.org/index.php/scpe>)
- ❖ implicarea studenților cu performanțe profesionale în activitatea de cercetare și creșterea nivelului calitativ al programelor de master și doctorat;
- ❖ promovarea infrastructurii de calcul de înaltă performanță, identificarea de potențiali utilizatori și identificarea unor noi direcții de cercetare care să exploateze infrastructură existentă.

7.3 Direcții și teme de cercetare

Direcțiile curente de cercetare ale grupurilor de cercetare din cadrul Centrului de Cercetare în Informatică:

- Calcul distribuit și calcul de înaltă performanță
 - Platforme pentru proiectarea și execuția aplicațiilor în cloud
 - Gestiunea în manieră autonomă a resurselor și guvernanta în cloud
 - Ingineria software a aplicațiilor bazate pe cloud
 - Securitate în cloud
 - Ontologii pentru proiectarea și regăsirea în manieră semantică a serviciilor software
 - Compunerea și orchestrarea serviciilor software
 - Calcul de tip transprecizie cu aplicațiilor în fog și edge computing
 - Prelucrarea volumelor mari de date
 - Accelerarea aplicațiilor folosind infrastructura hibridă (CPU, GPU)
 - Aplicații ale calculului de înaltă performanță în prelucrarea imaginilor, grafică, analiza datelor, proiectarea sistemelor de detecție a intrușilor
 - Aplicații în domeniul procesării datelor stelitare, în domeniul detecției anomaliilor și în implementarea tehnologiilor de tip blockchain
- Inteligență artificială și învățare automată
 - Sisteme multi-agent în rezolvarea problemelor complexe
 - Servicii inteligente și prelucrarea volumelor mari de date folosind calculul de înaltă performanță
 - Sisteme de recomandare și de asistare a deciziei bazate pe învățare automată cu aplicații în proiectarea, monitorizarea și distribuirea serviciilor software pe infrastructuri de tip cloud
 - Metaeuristici inspirate de natură cu aplicații în planificarea task-urilor în sisteme distribuite, auto-scalarea resurselor pentru aplicații cloud, estimarea parametrilor în modele din biologia computațională, analiza datelor etc.

- Aplicații ale rețelelor neuronale cu structură profundă în procesarea semnalelor, a imaginilor (imagini satelitare, imagini medicale) și analiza datelor de tip text.
- Aplicații ale tehnicilor de învățare automată în detecția de obiecte din imagini astronomice.
- Teoria calculului
- Metode combinatoriale și probabilistice în analiza sistemelor complexe;
 - Proiectarea și analiza algoritmilor aproximativi cu aplicații în modelarea rețelelor sociale și a celor biologice;
 - Aplicații ale teoriei jocurilor;
 - Programare logică și programare cu constrângeri;
 - Proprietăți ale limbajelor regulate, automate și sisteme de rescriere;
 - Demonstrare automată și sinteza algoritmilor.
- Matematici computaționale și aplicații
 - Analiza proprietăților ecuațiilor diferențiale cu ordin fracționar;
 - Analiza dinamicii rețelelor neuronale recurente;
 - Modele discrete și continue - stabilitate, control, bifurcații, haos;
 - Modele discrete și continue- aplicații în aeronautică și biologia computațională;
 - Aplicații ale modelele statistice în analiza datelor biologice;
 - Modele computaționale în domenii interdisciplinare (chimie, biologie).

Integrarea ocupantului postului în strategia de cercetare a Departamentului de Informatică.

Ocupantul postului scos la concurs trebuie să se integreze în unul dintre grupurile de cercetare existente sau să inițieze un nou grup de cercetare pe una dintre direcțiile strategice la nivel național și internațional în domeniul informaticii. Se așteaptă ca ocupantul poziției să obțină anual rezultate relevante în direcția de cercetare pe care activează și să contribuie la dezvoltarea expertizei din cadrul Centrului de Cercetare în Informatică.

8. Strategia de internaționalizare a departamentului/școlii doctorale și a programelor de studii gestionate de departament și modul în care ocupantul postului ar trebui să se integreze acestei strategii

Strategia de internaționalizare a Facultății de Matematică și Informatică se aliniază scopurilor și obiectivelor propuse în Strategia de Internaționalizare și Cooperare Globală a Universității de Vest din Timișoara vizează următoarele direcții principale:

ARIA STRATEGICĂ 1: INTERNAȚIONALIZAREA ACASĂ

Obiectivul 1.1 Organizare de evenimente internaționale

- Continuarea organizării evenimentelor științifice de tradiție (conferințele SYNASC, OT) și atragerea de evenimente noi (conferințe, workshop-uri, școli de vară) cu scopul de a facilita accesul studenților și al personalului didactic la evenimente internaționale – au fost organizate următoarele evenimente științifice:
 - Meeting on Program Verification – workshop în cadrul European Network on Formal Proof, COST Action CA20111, 8-9 februarie 2023 (<https://europroofnet.github.io/wg3-timisoara/>)
 - 5 workshop-uri în cadrul conferinței Smart Diaspora 2023, 10-13 aprilie 2023 (<https://www.info.uvt.ro/workshops-smart-diaspora-2023/>)
 - Abordări orientate către om pentru Inteligență Artificială de încredere
 - Bioinformatica fără frontiere: de la infrastructura de date la aplicații multidisciplinare
 - Engineering Responsible Smart Systems
 - Securitate cibernetică, criptanaliză cu metode cuantice și modele neconvenționale de calculabilitate
 - Matematica – motorul științei contemporane: viziune, metode, inovație
 - 25th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 11-14 septembrie 2023, Nancy, Franța (<https://synasc.ro/2023/>)
 - 37th RoMedINF Conference "Healthcare Green Digital Ecosystems: From Data Analysis to Digital Twin", 14-15 septembrie 2023 (<https://romedinf.srimed.ro/>)
- Participarea la competiții pentru organizarea unor evenimente științifice itinerante (cel puțin o competiție la fiecare 2 ani) – a fost depusă o propunere pentru găzduirea ediției din 2026 a European Conference on Computer Vision; propunerea este în prezent în evaluare
- Sprijinirea inițiativei „West University of Timisoara (Late) Summer School” prin ofertarea de cursuri pe tematici de actualitate din domeniul matematicii și informaticii (1-2 cursuri pe an) – nu au fost oferite cursuri în 2023

Obiectivul 1.2 Dezvoltare de programe de studii cu orientare și curriculum internațional

- Promovarea unor standarde ridicate de predare și evaluare și actualizarea continuă a ofertei curriculare în concordanță cu cea a universităților de prestigiu din lume – 3 noi programe de studii cu predare în limba engleză introduse în 2023:
 - Artificial intelligence (licență)
 - Cybersecurity (master, anterior în limba română)
 - Intelligent software robotics (master)
- Extinderea colaborării cu cadre didactice de la universități din străinătate pentru a susține activități didactice modulare la programele de studii cu predare în limba engleză – în corelare cu Obiectivele 1.3 și 6.1 – în semestrul 1 2023-2024, prof. Arpad Benyi (Visiting Lecturer @ UVT) a susținut cursul de Analiză Fourier pentru studenții de la programele de master din domeniul Matematică. De asemenea, au fost create 2 posturi în statul de funcții al Departamentului de Informatică pentru care sunt potențial vizati candidați internaționali. Acestea vor fi scoase la concurs în semestrul 2.

- Continuarea implicării în parteneriatul ECS (European Computer Science) – program de studii de tip diplomă dublă prin promovarea ofertei educaționale a Departamentului de Informatică în rândul partenerilor și prin încurajarea studenților de la programul de studii Informatică în limba engleză să urmeze anul III la una dintre instituțiile partenere (în medie 2 studenți outgoing și 4 studenți incoming pe an)
 - 2022-2023 – 2 studenți incoming, 1 outgoing
 - 2023-2034 – 3 studenți incoming
- Asigurarea cadrului pentru creșterea numărului de doctorate în co-tutelă (10% din tezele de doctorat care vor fi susținute în cinci ani să fie elaborate în co-tutelă internațională) –

Obiectivul 1.3 Visiting@UVT

- Atragerea de personal academic cu recunoaștere internațională prin intermediul programului de granturi Visiting@UVT pentru desfășurarea de activități didactice și de cercetare în cadrul Facultății de Matematică și Informatică (minim 1 poziție Visiting Scholar ofertată/an universitar)
 - Semestrul 2 2022-2023 – 1 Visiting Researcher (dr. Anca Ruxandra Rădulescu, Associate Professor la State University of New York at New Paltz, USA)
 - Semestrul 1 2023-2024 – 1 Visiting Lecturer (dr. Arpad Benyi, Professor la Western Washington University, USA) și 1 Visiting Researcher (dr. Argha Mondal, Assistant Professor la Sidho-Kanho-Birsha University, India)
 - Semestrul 2 2023-2024 – selecție finalizată - 1 Visiting Researcher (dr. Anca Ruxandra Rădulescu)

Rezultate: crearea de cursuri noi, materiale didactice, intensificarea colaborărilor în domeniul cercetării.

Obiectivul 1.4 Dezvoltarea și consolidarea competențelor de comunicare în limbi de circulație internațională pentru personalul Facultății de Matematică și Informatică

- Participarea personalului administrativ și didactic la cursuri de limbi străine organizate de UVT – există interes în rândul personalului suport pentru cursuri de limba engleză/franceză orientate pe limbaj de tip administrativ
- Promovarea în rândul tinerilor cercetători a cursurilor de scriere academică în limba engleză (minim 1 eveniment/an universitar) –

ARIA STRATEGICĂ 2: STUDENȚI INTERNAȚIONALI ȘI MARKETING GLOBAL

Obiectivul 2.1 Recrutarea, admiterea și școlarizarea studenților internaționali

- Atragerea de studenți internaționali, în special la programele de studii cu predare în limba engleză, prin acțiuni de promovare a acestor programe (pachet de materiale promoționale în limba engleză, informații relevante ușor accesibile pe pagina web a facultății, traducerea în engleză a planurilor de învățământ, publicarea lor și comunicarea constantă către responsabilii Departamentului de Relații Internaționale) - comunicare constantă cu DRI pentru actualizarea informațiilor despre programele de studii în limbi străine în scopul promovării acestora

Studenți internaționali licență și master:

- 2021-2022: 69 din 1726 (4%)
- 2022-2023: 82 din 1580 (5.2%)
- 2023-2024: 90 din 1634 (5.5%)
- Prezența la târguri internaționale de recrutare împreună cu personalul Departamentului de Relații Internaționale pentru a oferi candidaților detalii și răspunsuri la întrebări specifice programelor vizate (1-2 evenimente/an) – participare FMI la International Global Open Day@WUT

Obiectivul 2.2 Creșterea vizibilității în mediul online

- Actualizarea periodică a informațiilor disponibile pe versiunea în limba engleză a paginii web a facultății și promovarea pe această cale a rezultatelor notabile obținute de către cadre didactice și studenți – site web actualizat
- Participarea în clasamente internaționale de referință – furnizarea informațiilor solicitate de către departamentele de resort ale UVT pentru includerea în clasamente internaționale

ARIA STRATEGICĂ 3: ERASMUS

Obiectivul 3.1 Creșterea numărului și a calității mobilităților de studii, plasament, predare și formare

- Creșterea progresivă (cu minim 5%/an) a numărului de mobilități fizice și virtuale efectuate de studenți în țări ale UE, cât și în țări din afara Uniunii Europene, prin programele Erasmus+, SEE, CEEPUS, DAAD și alte acorduri bilaterale și încurajarea, pe cât posibil, a principiului reciprocității referitor la studenți incoming/outgoing
 - 2021-2022: 22 mobilități studenți incoming și 19 outgoing
 - 2022-2023: 23 mobilități studenți incoming și 18 outgoing
 - 2023-2024: 25 mobilități studenți incoming și 9 outgoing pe semestrul I
- Încurajarea cadrelor didactice din facultate să efectueze stagii de cercetare și predare la universități de prestigiu din străinătate
 - 2021-2022: 6 mobilități outgoing
 - 2022-2023: 10 mobilități outgoing
 - 2023-2024: 1 mobilitate outgoing realizată, alte 6 prevăzute pentru 2024, există interes pentru mobilități suplimentare
- Organizarea de evenimente de promovare, în care beneficiarii ai acestor programe de mobilități își împărtășesc experiența în cadrul programului (1 eveniment pe an pentru studenți, 1 eveniment pe an pentru cadre didactice) - participare la evenimentele organizate în acest scop la nivel UVT

Obiectivul 3.2 Alte proiecte Erasmus

- Stimularea depunerii de aplicații pentru diferite proiecte finanțate prin Erasmus, inclusiv prin premiarea, prin mecanismul de acordare a salariilor diferențiate, a depunerii unui proiect Erasmus+ care a fost declarat nefinanțabil, dar a obținut un punctaj de minim 75% din punctajul proiectului situat pe prima poziție în clasamentul final al competiției respective (ținta este derularea în cadrul Facultății de Matematică și Informatică a cel puțin 1 proiect educațional Erasmus+/ an universitar) – a fost demarat proiectul

Erasmus+ Parteneriate de Cooperare pentru Învățământ Universitar KA220-HED-000152418 *AiRobo: Artificial Intelligence based Robotics* – coordonator: Universitatea de Vest din Timisoara (conf. dr. Isabela Drămnesc), parteneri: Universitatea Macedonia, Thessaloniki, Grecia, Universitatea Esztherhazy Karoly, Eger, Ungaria, Universitatea RWTH Aachen, Germania, Universitatea Lorraine, Metz, Franta; perioada de implementare: 1.12.2023 - 30.11.2026

ARIA STRATEGICĂ 4: UNIVERSITATEA EUROPEANĂ UNITA

Obiectivul 4.1 Promovarea valorilor, obiectivelor și acțiunilor consorțiului UNITA în cadrul comunității de cadre didactice și studenți

- Promovarea mobilităților fizice și virtuale, pentru cadre didactice și studenți, în cadrul consorțiului UNITA – 8 studenți cu mobilitate Erasmus incoming de la universități din UNITA în 2023-2024
- Identificarea de direcții comune de cercetare și dezvoltarea de parteneriate și proiecte de cercetare în cadrul consorțiului
 - s-a inițiat o colaborare în domeniul bioinformaticii cu un grup coordonat de prof.dr. Santana Cutrupi de la Universitatea din Torino; în acest context dr. Alexandru Mizeraschi (ICAM) a efectuat un stagiu de o lună la Universitatea din Torino pe tematica "Networking RNA binding proteins in alternative splicing"
 - au fost demarate discuții cu cercetători de la Universitatea din Zaragoza care activează în domeniul human computer interfaces; este în lucru o propunere de proiect în cadrul unui apel european
 - s-a inițiat o discuție cu partenerii de la Univ. Torino, Univ. Savoie Mont Blanc, Univ. Pau et Pays de l'Adour, Univ. Transilvania Brașov cu scopul organizării unor activități/programe de studiu în colaborare. Se vizează organizarea unui program de master cu diplomă comună/multiplă cu tematica *Data Centric Technologies* și s-a propus o structura preliminară a programului. De asemenea, s-a definit un concept de colaborare în cadrul disciplinelor orientate spre activități practice (practică de cercetare, practică profesională, proiecte în colaborare cu industria): *International Collaborative Applied Research in Data Centric Technologies (ICARE)* și s-a stabilit un calendar de activități pentru a putea fi pus în practică începând cu anul universitar 2024-2025

ARIA STRATEGICĂ 5: INTERNAȚIONALIZAREA CERCETĂRII

Obiectivul 5.1 Evenimente și proiecte de cercetare internaționale

- Accesarea și implementarea de proiecte de cercetare cu parteneri internaționali, pentru a spori vizibilitatea facultății și a UVT pe piața cercetării academice internaționale (cel puțin 2 proiecte internaționale derulate în următorii 5 ani)
 - SYMSAFE - Symbolic rewriting methods for safety and security of critical cyber-physical systems, 2023-2026, Science for Peace and Security Programme, NATO Emerging Securities Challenges Division, proiect nr. G6133 (M. Marin)

- HARMONIA - Development of a Support System for Improved Resilience and Sustainable Urban areas to cope with Climate Change and Extreme Events based on GEOSS and Advanced Modelling Tools, H2020-LC-CLA-2020-2/RIA, 2021-2024 (M. Neagul, C. Bonchiș)
- SERRANO – Transparent Application Deployment in a Secure, Accelerated and Cognitive Cloud Continuum, H2020/RIA, 2021-2023 (S. Panica)
- EuroProofNet - European Network on Formal Proof, COST Action CA20111, 2022-2026
- HiTeC - Text, functional and other high-dimensional data in econometrics: new models, methods, applications, COST Action CA21163, 2022-2026
- Susținerea financiară a participării cadrelor didactice și tinerilor cercetători la conferințe internaționale de mare vizibilitate și a mobilităților internaționale pentru colaborare în domeniul cercetării – 84 deplasări internaționale realizate în 2023, pe lângă mobilitățile Erasmus deja menționate la punctul 3.1:
 - Cadre didactice: 53 (participări la conferințe, vizite de cercetare, întâlniri ale echipelor de proiecte de cercetare, întâlniri ale organizațiilor profesionale, evenimente de networking, participare în comisii de teze de doctorat)
 - Studenți, masteranzi și doctoranzi: 31 (participări la conferințe, workshop-uri, școli de vară, stagii de cercetare, concursuri studențești)

Finanțarea acestor deplasări s-a făcut din proiecte de cercetare, FDI, FSS, granturi Develop, respectiv venituri proprii FMI.

- Invitarea de cercetători (inclusiv membri ai Diasporei) care își desfășoară activitatea la instituții din străinătate pentru a susține prelegeri în cadrul evenimentelor organizate în cadrul facultății sau al seminariilor științifice (cel puțin 5 pe an) – o prelegere în cadrul seriei de evenimente Diaspora@WUT Guest Lectures (a se vedea Obiectivul 6.2), 13 prelegeri ale unor cercetători din străinătate în cadrul seminariilor științifice:
 - Arpad Benyi, Western Washington University, USA (Visiting Lecturer @ UVT)
 - Argha Mondal, Department of Mathematics, Sidho-Kanho-Birsha University, India & University of Essex, UK (Visiting Researcher @ UVT)
 - Thomas Strobl, Claude Bernard University Lyon, Franța
 - Konstanze Rietsch, King's College London, UK
 - George Lusztig, MIT, USA
 - Alina Lazăr, Youngstown State University, USA
 - Ivan Stajduhar, University of Rijeka, Croația
 - Boris Naujoks, Cologne University of Applied Sciences, Germania
 - Sorin Stratulat, University of Lorraine, Franța
 - Anabela Gomes, University of Coimbra, Portugalia
 - Leonor Melo, University of Coimbra, Portugalia
 - Damiano Di Francesco Maesa, University of Pisa, Italia
 - Federico Della Croce, DIGEP Politecnico di Torino, Italia

Obiectivul 5.2 Publicații internaționale

- Stimularea creșterii continue a numărului de articole științifice publicate în cooperare cu parteneri internaționali (se vizează atingerea unei medii de 40 publicații indexate Web

of Science în colaborare cu parteneri afiliați unor instituții din străinătate/2 ani), inclusiv prin premiarea suplimentară a publicațiilor de acest tip indexate Web of Science prin intermediul salariilor diferențiate – metodologie salarii diferențiate actualizată din 2022 pentru premiere suplimentară publicații cu parteneri internaționali, 15 publicații în reviste indexate ISI în colaborare cu parteneri afiliați unor instituții din străinătate în 2020, 22 în 2021, 17 în 2022, 16 în 2023 până în prezent

- Sprijinirea Analelor Universității de Vest din Timișoara, Seria Matematică – Informatică pentru includerea în fluxul publicațiilor indexate Scopus sau ISI Web of Science – continuitate în publicare AWUTM (1 fascicul în 2023 în format Volume Open), analiză criterii pentru indexare AWUTM în Scopus

ARIA STRATEGICĂ 6: DIASPORA ROMÂNĂ

Obiectivul 6.1 Dezvoltarea rețelei UVT – Diaspora Română

- Crearea unei baze de date de absolvenți ai FMI ce activează în prezent în domeniul academic sau de cercetare peste hotare și promovarea către aceștia a evenimentelor și acțiunilor organizate de către facultate – actualizare bază de date creată de DRI
- Identificarea de noi oportunități de colaborare cu cercetători din Diaspora Română, cum ar fi organizarea de evenimente științifice comune (de exemplu continuarea organizării Romanian Algorithms Days) – 5 workshop-uri în cadrul conferinței Smart Diaspora 2023 (a se vedea Obiectivul 1.1)

Obiectivul 6.2 Organizarea de evenimente dedicate colaborării cu Diaspora Română

- Organizarea anuală în cadrul FMI a evenimentului Romanian Diaspora Guest Lecture - prelegere Diaspora@WUT – Prof. univ. dr. Florin Rădulescu (Universită degli Studi di Roma "Tor Vergata", Italia), 19.09.2023

9. Fișa individuală a postului ce urmează a fi scos la concurs, respectiv pentru care urmează să se organizeze examen de promovare, după caz, care include descrierea postului și atribuțiile/activitățile aferente postului scos la concurs, respectiv pentru care se organizează examen de promovare, după caz. În cazul posturilor de cercetare din cadrul departamentelor academice ale UVT vacante scoase la concurs, fișa individuală a postului va conține și indicatori de cercetare clar definiți și cuantificați

Anexa 1

10. Fișele disciplinelor incluse în post

Anexa 2 - include fișele disciplinelor *Proiect colectiv* și *Securitate și criptografie, Operating systems I* și *Cryptography and information security*

11. Salariul minim de încadrare

Conform informațiilor primite de la Resurse umane, adresa **SALARIILE DE ÎNCADRARE** aferente posturilor didactice și de cercetare din învățământul superior, scoase la concurs în anul universitar 2024-2025, cu numărul Nr. 64013/23.09.2024 salariul pentru Lector universitar, tranșa 3-5 ani, gradație 1 7.246 lei(*Anexa 3*)

12. Extras din statul de funcții care să evidențieze postul vacant scos la concurs sau pentru care se organizează examen de promovare în cariera didactică, după caz

Anexa 4 - Statul de funcții 2024 - 2025 al departamentului de Informatică paginile 7-8.

13. Programa aferentă concursului/examenului de promovare în cariera didactică – tematica probelor de concurs/examen

Proiect colectiv

- Metode, tehnici și instrumente utilizate în managementul proiectelor
- Verificarea și validarea etapelor de realizare a Proiectului Colectiv
- Elaborarea, prezentarea și validarea livrabilelor realizate în Proiectul Colectiv

Securitate și criptografie

- Concepte de securitate și criptografie.
- Clasificarea metodelor de criptare. Criptografie clasică și tendințe actuale în criptografie și analiza criptografică
- Criptarea convențională clasică. Modelul criptării convenționale
- Algoritmi de cifrare clasici (Codul lui Caesar, Roata alfabetică, Tabele Viginere, Tabela Porta, Codificări matrice, Codificări Bifid, Codificări cu transpoziție, Codul Playfair, Codul Hill)
- Algoritmi moderni de criptare. Principiile codurilor bloc. Structura codului Feistel. Algoritmii: DES, Triplu DES, IDEA, RC5, AES
- Criptarea cu chei publice. Algoritmul RSA. Algoritmul Diffie-Hellman
- Funcții hash, semnături digitale.
- Administrarea cheilor
- Tehnici de atac și apărare în era internetului.
- Criptarea cuantică

Operating systems I

- Introduction. History. Generations of Operating Systems. The evolution of basic concepts; The Computing System: the processor, the memory, I/O devices, system bus; Structure of (modern) computing systems: monolithic, layered, virtual machines, client-server.
- Fundamentals. Basic notions: processes, deadlock, memory management, I/O devices, security; System calls: process management, file and directory management, other system calls. Hardware components of a computing system; Mapping of hardware components on basic operating systems concepts.
- Processes and threads. Process description and process control. Process model; Creation and termination of processes; Process states. Hierarchies of processes; Information about processes, cooperating processes, process scheduling. Threads; Threads description and control. Usage of threads; Threads implementation. Threads in user space, threads in kernel space, pop-up threads, mixed approach; Typical problems in thread usage.
- Inter-process communication (IPC). Basis of IPC communication: race conditions, critical regions, mutual exclusion, busy waiting. Mutual exclusion. Solutions for busy waiting: interrupt deactivation, strict alternation, TSL instruction, lock variables etc.; Synchronizing execution: sleep/wakeup, semaphores, mutex, monitores, barriers, message passing. Classical problems of inter-process communication. The dining philosophers; Readers and writers; Barbershop; Consumer-producer. Implications of these problems in modern operating systems.
- Process scheduling. Scheduling. General information. Scheduling in different operating systems. Goals of scheduling; Scheduling in batch-processing systems; Scheduling in interactive systems; Threads scheduling.
- Deadlocks. Preemptive and non-preemptive resources, resource acquisition, deadlock conditions, deadlock modeling; Ostrich algorithm; Detection, avoidance, prevention of deadlocks. Algorithms for deadlock detection, avoidance, prevention; Banker's algorithm
- Memory management. Basic notions. Monoprogramming and multiprogramming; Memory relocation and memory protection; Swapping. Memory management (swapping based); Virtual memory. Pagination, page tables.
- Memory management. Page replacement algorithms; Modeling page replacement algorithms; Requirements for the implementation of memory management; Segmentation.

Cryptography and information security

- Case study: Breaking down modern depictions of Information Security examples and hacking breaches
- Good practices for securing data. Definition of security: IND-CPA. History of cryptography

- Trapdoor functions. RSA, trapdoor permutations and another public-key cryptosystem.
- QRA, Goldwasser-Micali and Homomorphism.
- Digital Signatures: Definition. Lamport's One-time Signature Scheme.
- Collision-resistant hash functions. Many-time, stateful, signature schemes. Naor-Yung construction: stateless EUF-CMA-secure signature schemes.
- Instantiation of collision-resistant hash functions from discrete log. Direct construction of digital signatures from RSA. The hash-and-sign paradigm and the random oracle heuristic. Variants of digital signatures.
- Zero knowledge I, definitions and examples. Zero Knowledge Proofs for all of NP.
- Succinct (Zero Knowledge) Argument Systems. Tools: Merkle Trees, Probabilistically Checkable Proofs . Kilian's Protocol.
- Lattices, Learning with Errors (LWE). LWE-based Cryptography: Secret-key and Public-key Encryption, Collision-Resistant Hashing. Fully Homomorphic Encryption. A Construction of FHE from the LWE assumption.
- Fully Homomorphic Encryption continued: The Bootstrapping Theorem, and Circular Security. Open Problems in FHE Research.
- Oblivious Transfer. Private Information Retrieval.
- Secure Two-Party Computation. The Goldreich-Micali-Wigderson Protocol.
- Secret-Sharing. Secure Multiparty Computation.
- Program Obfuscation and Applications.

14. Extrase din procesele verbale ale ședinței Consiliului departamentului și ședinței Consiliului facultății în care au fost aprobate aceste poziții

Anexa 5 - Extrasul din procesul verbal al ședinței Consiliului Departamentului de Informatică

Anexa 6 - Extrasul din procesul verbal al ședinței Consiliului Facultății de Matematică și Informatică.

Data

Semnătura directorului de departament

12.03.2025

Lector Dr. Adriana Loredana Tănasie

Aprobat, *Prof. Univ. Dr.*
Marilen Gabriel PIRTEA

FIȘA POSTULUI
personal didactic

Anexă la Contractul Individual de Muncă nr. ...

I. DATE PRIVIND IDENTIFICAREA POSTULUI

1. Numele și prenumele titularului:
2. Facultate: **Matematică și Informatică**
3. Departament: **Informatică**
4. Denumirea postului: **LECTOR UNIVERSITAR** / Cod COR: **231003**

II. CONDIȚII SPECIFICE PRIVIND OCUPAREA POSTULUI

1. Studii specifice: superioare, conform Legislației și Regulamentului de ocupare a posturilor didactice
2. Experiență: conform Regulamentului de ocupare a posturilor didactice
3. Competență managerială¹ (cunoștințe de management, calități și aptitudini manageriale)

4. SFERA RELAȚIILOR ORGANIZAȚIONALE

1. Ierarhice:
 - subordonat față de: **DIRECTOR DEPARTAMENT**
 - superior pentru: -
2. Funcționale: cadre didactice, departamentele administrative, organizații studențești;
3. Reprezentare: -
4. Sfera relațională:
 - internă - cu cadre didactice, departamentele administrative, organizații studențești;
 - externă - cu reprezentanți ai organismelor partenere Departamentului/Facultății/Universității de Vest din Timișoara.

IV. OBIECTIVELE SPECIFICE POSTULUI

Desfășurarea activităților didactice, de cercetare și a celor complementare, în concordanță cu misiunea și obiectivele Universității de Vest din Timișoara, urmărindu-se creșterea calității prestației didactice, a rigorii științifice, precum și perfecționarea pregătirii profesionale.

V. ATRIBUȚII, RESPONSABILITĂȚI ȘI SARCINI SPECIFICE POSTULUI

A. Activități normate în statul de funcții

I. Activități de predare, inclusiv pregătirea acestora

1. Cursuri aferente ciclului de studii universitare de licență
2. Cursuri aferente ciclului de studii universitare de master

¹ Pentru funcțiile de conducere

3. Cursuri la forma studii academice postuniversitare
4. Cursuri la forma studii postuniversitare de specializare, inclusiv cursuri de pregătire pentru examenele de definitivat sau dobândirea de grad didactic organizate pentru profesorii din licee, gimnazii și pentru institutori
5. Cursuri de perfecționare postuniversitare, inclusiv cursuri de pregătire pentru examenele de definitivat sau dobândirea de grad didactic organizate pentru profesorii din licee, gimnazii și pentru institutori
6. Module de curs pentru formarea continuă
7 ² . Cursuri la școlile de studii avansate (doctorate)
8 ³ . Cursuri organizate pentru pregătirea doctoranzilor
9. Alte cursuri (prelegeri) normate la forme moderne de învățământ universitar
II. Activități de seminar, proiecte de an, lucrări practice și de laborator (inclusiv pregătirea acestora)
1. Activități de seminar, complementare sau nu cursurilor enumerate la capitolul A.I., după caz, conform planului de învățământ
2. Îndrumarea realizării proiectelor de an, complementare sau nu cursurilor de la capitolul A.I., după caz, conform planului de învățământ
3. Lucrări practice și de laborator, conform cu planul de învățământ;
III. Îndrumarea (conducerea) proiectelor de finalizare a studiilor, a lucrărilor de licență și de absolvire (disertație)
IV. Îndrumarea (conducerea) de proiecte de absolvire, de lucrări de disertație sau de absolvire pentru toate formele de pregătire postuniversitară, prevăzute în planul de învățământ
V. Activitate de practică productivă sau practică pedagogică (inclusiv pregătirea acestora)
VI ⁴ . Îndrumarea doctoranzilor în stagiul (activitate normată) și în poststagiul
VII. Conducerea activităților didactice artistice sau sportive (inclusiv pregătirea acestora) ⁵
1. Cursuri de turism pentru studenți
2. Cursuri sportive pentru studenți sau copiii angajaților
3. Gimnastică aerobică
4. Antrenamente cu echipe reprezentative (atletism, jocuri sportive)
5. Îndrumarea loturilor sportive în timpul desfășurării competițiilor
6. Organizarea de crosuri sau alte manifestări sportive de interes universitar sau național
7. Îndrumarea formațiilor artistice de interes universitar
8. Organizarea manifestărilor artistice
VIII. Activități de evaluare
1. Evaluare în cadrul pregătirii prin doctorat ⁶ :
- Comisie concurs de admitere
- Comisie examen de doctorat
- Comisie susținere publică teza de doctorat, inclusiv de evaluare a tezei
- Evaluare referat de doctorat (prin participare la comisia de îndrumare)
2. Evaluare în cadrul concursurilor de admitere la toate formele de învățământ (inclusiv postuniversitar, altele decât doctoratul):
- Elaborare tematică și bibliografie
- Comisie redactare subiecte
- Comisie examinare orală
- Comisie corectură teze
- Corectură teste
- Comisie supracorectură

² Dacă nu se regăsesc în Statul de funcții de la Școala doctorală

³ Dacă nu se regăsesc în Statul de funcții de la Școala doctorală

⁴ Dacă nu se regăsesc în Statul de funcții de la Școala doctorală

⁵ În cazul facultăților de profil (Facultatea de Arte și Design, Facultatea de Educație Fizică și Sport, respectiv Facultatea de Muzică și Teatru)

⁶ Dacă nu se regăsesc în Statul de funcții de la Școala doctorală

<ul style="list-style-type: none"> - Comisie contestații - Comisie concurs de admitere (organizare, modernizare) - Comisie supraveghere examen scris <p>3. Evaluarea în cadrul activităților didactice directe la toate formele de învățământ (curs, seminar, proiecte de an, proiecte (lucrări) de finalizare a studiilor, lucrări de laborator) inclusiv:</p> <ul style="list-style-type: none"> - Evaluare și notare teme de casă/proiecte - Evaluare și notare examene parțiale - Evaluare și notare examen (test) final - Evaluare și notare teme (probleme) rezolvate acasă <p>4. Evaluare și activități complementare în cadrul comisiilor de finalizare a studiilor universitare sau postuniversitare</p> <ul style="list-style-type: none"> - Elaborare tematică și bibliografie - Comisie elaborare subiecte - Comisie examinare și notare - Comisie supraveghere probe scrise - Comisie corectură (supracorectură) - Comisie contestații
IX. Consultații (pentru toate formele conexe cursurilor de la capitolul A.I.)
X. Îndrumarea cercurilor științifice
XI. Îndrumarea studenților (tutoriat) pentru alegerea rutei profesionale în cadrul sistemului de credite transferabile
XII. Participarea la comisii și consilii în interesul învățământului
<p>XIII. Activități privind promovarea cadrelor didactice din învățământul preuniversitar</p> <p>1. Definitivatul</p> <ul style="list-style-type: none"> - Elaborare programe și bibliografie - Îndrumare și consultanță de specialitate și pedagogică - Inspecție școlară specială pentru evaluarea de specialitate, metodică și pedagogică - Elaborarea subiectelor pentru probele scrise, supraveghere, corectare și notare - Elaborarea subiectelor pentru probele orale, examinare și notare (comisie) - Organizare examen <p>2. Gradul didactic II</p> <ul style="list-style-type: none"> - Elaborare programe și bibliografie - Consultanță și îndrumare (minimum două inspecții) - Inspecție școlară specială pentru evaluarea de specialitate, metodică și pedagogică - Elaborarea subiectelor pentru testul de specialitate și metodică specialității - Supraveghere teză, corectare și notare - Elaborarea subiectelor pentru proba orală, examinare și notare <p>3. Gradul didactic I</p> <ul style="list-style-type: none"> - Elaborare tematică, elaborare subiecte, examinare și notare în cadrul colocviului de admitere - Îndrumare (minimum două inspecții) - Inspecție școlară specială pentru evaluarea de specialitate, metodică și pedagogică - Îndrumarea și evaluarea lucrării metodică-științifice - Participare la comisia pentru susținerea lucrării de grad (evaluare și notare) <p>4. Concurs pentru ocuparea posturilor vacante</p> <ul style="list-style-type: none"> - Elaborarea tematicii și a bibliografiei - Comisie susținere examen - Comisie contestații - Comisie organizare concurs - Comisie supraveghere probe scrise
<p>XIV. Activități privind pregătirea și promovarea cadrelor didactice din învățământul superior</p> <p>1. Concurs pentru ocuparea unui post de asistent universitar</p> <ul style="list-style-type: none"> - Îndrumare metodică și științifică - Elaborare tematică și bibliografie

<ul style="list-style-type: none"> - Elaborarea subiectelor pentru probele scrise, supraveghere teză, corectare și notare - Elaborarea subiectelor pentru probele orale, examinare și notare - Participare la proba practică și evaluare <p>2. Concurs pentru ocuparea unui post de lector universitar (șef de lucrări)</p> <ul style="list-style-type: none"> - Îndrumare metodică și științifică - Verificare dosar de concurs - Stabilire temă prelegere - Participare la prelegere publică - Evaluare <p>3. Concurs pentru ocuparea unui post de conferențiar universitar sau profesor universitar</p> <ul style="list-style-type: none"> - Analiză de dosar - Stabilire temă prelegere - Participare la prelegerea publică - Evaluare
--

B. Activități de pregătire științifică și metodică și alte activități în interesul învățământului

I. Pregătire individuală (autoperfecționare)
II. Audierea unor cursuri sau parcurgerea unor module de curs. Parcurgerea completă a formelor postuniversitare de învățământ în domeniul de activitate sau într-unul complementar
III. Participarea la conferințe, simpozioane, congrese ș.a., organizate în domeniul de activitate principal sau în domenii interdisciplinare
IV. Organizarea de congrese ș.a., în domeniul de activitate sau în domenii colaterale (complementare)
V. Înființarea, amenajarea și modernizarea laboratoarelor, a stațiilor-pilot, a centrelor de excelență (cercetare), a aparatului de laborator ș.a.
VI. Organizarea de schimburi academice între diferite universități din țară și din străinătate
VII. Participarea la programele internaționale la care România este parte
VIII. Perfecționarea propriei pregătiri pedagogice
IX. Elaborarea de manuale, îndrumare, culegeri de probleme și de teste și a altor materiale didactice

C. Activități de cercetare științifică, de dezvoltare tehnologică, activități de proiectare, de creație artistică potrivit specificului

I. Activități prevăzute în planul intern
II. Activități în cadrul centrelor de cercetare din cadrul UVT
III. Activități în cadrul centrelor de transfer tehnologic
IV. Elaborarea individuală de inovare sau invenție prevăzute în planul intern
V. Documentare privind oportunitățile de finanțare pentru proiecte de cercetare
VI. Elaborarea tratatelor, a monografiilor și a cărților de specialitate prevăzute în planul intern

VI. ALTE SARCINI ȘI RESPONSABILITĂȚI

I. Atribuții pe linie managerială și a celor cu privire la sistemul de control managerial intern, așa cum sunt ele stipulate în reglementările interne ale Universității de Vest din Timișoara în ceea ce privește dezvoltarea sistemului de control intern managerial.
II. Respectarea prevederilor Cartei, Regulamentelor și celorlalte reglementări interne în vigoare în Universitatea de Vest din Timișoara;
III. Respectarea obligațiilor privind prevenirea și protecția în domeniul securității și sănătății în muncă, prevenirea și apărarea împotriva incendiilor, așa cum sunt ele stabilite prin legislația din domeniu;
IV. Constituie obligație de serviciu verificarea zilnică (cu excepția concediului legal) a corespondenței electronice sosite pe adresa instituțională de e-mail;
V. Participarea, la solicitarea Directorului de Departament/Decanului, la alte activități în interesul instituției;
VI. Răspunde în termen la solicitările de ordin administrativ, punând la dispoziția persoanelor responsabile, documentele, datele și informațiile solicitate, legate de activitățile în care acesta este implicat.

VII.	Verificarea zilnică (cu excepția vacanțelor și a concediului legal) a corespondenței electronice sosite pe adresa instituțională de e-mail.
VIII.	În temeiul prevederilor art.39. alin. (2), lit.e) din Codul Muncii- republicat și a art.39. din Hotărârea nr. 355/2007 privind supravegherea sănătății lucrătorilor, salariatul este obligat să se prezinte la examenele medicale de supraveghere a sănătății la locul de muncă, conform planificării efectuate de către medicul de medicina muncii cu acordul angajatorului.
IX.	Se obligă să respecte secretul de serviciu.
X.	Asigură confidențialitatea datelor personale pe care le prelucrează pe toată durata contractului individual de muncă și după încetarea acestuia, pe termen nelimitat, în conformitate cu prevederile Regulamentului UE 2016/679, a altor dispoziții de drept al Uniunii Europene sau de drept intern, aplicabile.
XI.	Constituie obligație de serviciu și alte sarcini date de șeful ierarhic superior, legate de specificul postului cu respectarea repartizării echitabile a sarcinilor între posturi.
XII.	Realizarea sarcinilor de ordin administrativ reglementate la nivelul universității sau atribuite de șeful ierarhic superior; legate de specificul postului cu respectarea repartizării echitabile a sarcinilor între posturi.
<i>– se pot detalia alte sarcini, atribuții, responsabilități, obiective și/sau termene stabilite nominal de către șeful ierarhic superior;</i>	

VII. RESPONSABILITĂȚI PRIVIND PROTECȚIA ÎN DOMENIUL SECURITĂȚII ȘI SĂNĂTĂȚII ÎN MUNCĂ

- În realizarea sarcinilor de serviciu are obligația de a respecta Normele de Tehnica Securității și Sănătății Muncii și P.S.I.;
- Trebuie să își desfășoare activitatea, în conformitate cu pregătirea și instruirea sa, precum și cu instrucțiunile primite din partea șefului ierarhic superior astfel încât să nu expună la pericol de accidentare sau îmbolnăvire profesională atât propria persoană, cât și alte persoane care pot fi afectate de acțiunile sau omisiunile sale în timpul procesului de muncă;
- Să utilizeze corect mașinile, aparatura, uneltele, substanțele periculoase, echipamentele de transport și alte mijloace de producție;
- Să utilizeze corect echipamentul individual de protecție acordat și, după utilizare, să îl înapoieze sau să îl pună la locul destinat pentru păstrare;
- Să nu procedeze la scoaterea din funcțiune, la modificarea, schimbarea sau înlăturarea arbitrară a dispozitivelor de securitate proprii, în special ale mașinilor, aparaturii, uneltelor, instalațiilor tehnice și clădirilor, și să utilizeze corect aceste dispozitive;
- Să comunice imediat șefului ierarhic superior și/sau lucrătorilor desemnați orice situație de muncă despre care au motive întemeiate să o considere un pericol pentru securitate și sănătate, precum și orice deficiență a sistemelor de protecție;
- Să aducă la cunoștință șefului ierarhic superior accidente suferite de propria persoană;
- Să coopereze cu angajatorul și/sau cu lucrătorii desemnați, atât timp cât este necesar, pentru a face posibilă realizarea oricăror măsuri sau cerințe dispuse de către inspectorii de muncă și inspectorii sanitari, pentru protecția sănătății și securității lucrătorilor;
- Să coopereze, atât timp cât este necesar, cu angajatorul și/sau cu lucrătorii desemnați, pentru a permite angajatorului să se asigure că mediul de muncă și condițiile de lucru sunt sigure și fără riscuri pentru securitate și sănătate, în domeniul său de activitate;
- Să își însușească și să respecte prevederile legislației din domeniul securității și sănătății în muncă și măsurile de aplicare a acestora;
- Să dea relațiile solicitate de către inspectorii de muncă și inspectorii sanitari.

VIII. DELEGAREA

Delegarea atribuțiilor aferente postului se face doar temporar, cu respectarea reglementărilor interne privind redistribuirea sarcinilor de serviciu în caz de absență a unui angajat, cu aprobarea scrisă a Directorului de departament, nominalizându-se persoana înlocuitoare.

IX. EVALUAREA PERFORMANȚELOR

Performanța cadrelor didactice se evaluează pe baza componentelor prevăzute în Manualul calității (evaluarea activității didactice făcută de studenți, evaluarea colegială, evaluarea ierarhică, autoevaluare), precum și în concordanță cu indicatorii prevăzuți în strategiile de învățământ și cercetare elaborate la nivel instituțional și cu cei folosiți în evaluările la nivel național, obiectivul de performanță fiind „Bine”.

Activitățile prevăzute la punctul V (A) sunt normate în conformitate cu statele de funcții aprobate, în speță cu poziția aferentă postului ocupat.

Ponderea, cuantificarea și numărul de ore alocate activităților prevăzute la punctul V (A,B și C) și VI se pot modifica, fiind propuse de directorii de departament, avizate de consiliul facultății și aprobate de senatul universității, anual cu respectarea legilor în vigoare, inclusiv al Legii nr. 1/2011.

Angajatului îi revine obligația să realizeze activitățile prevăzute la punctul V, în conformitate cu clauza art.287, alin . 22 din Legea 1/2011 precum și cu clauza “durata muncii” din contractul individual de muncă, adică suma totală a orelor de muncă, realizată prin cumularea ponderilor activităților, este de 40 ore pe săptămână.

Ponderea individuală a activităților care nu sunt prevăzute în statele de funcții poate varia de la o lună la alta, pontajul/borderoul de prezență fiind verificat și avizat de către directorul de departament.

Nu fac obiectul normării activitățile, inclusiv cele de cercetare științifică, finanțate și angajate pe bază de contract cu alți beneficiari decât Ministerul Educației Naționale, Cercetării Științifice sau instituțiile de învățământ aflate în subordinea sa, sau prevăzute expres în fișele de post aferente altor contracte individuale de muncă încheiate de angajat cu Universitatea de Vest din Timișoara.

Această fișa de post nu include activitățile și responsabilitățile aferente funcțiilor didactice de conducere.

Director Departament

Decan Facultate

Semnatura _____

Semnatura _____

Departament Resurse Umane

Titular post

Semnatura _____

Semnatura _____

Data:

SYLLABUS

1. Information about the study programme

1.1 Institution of higher education	West University of Timișoara
1.2 Faculty	Mathematics and Informatics
1.3 Department of	Informatics
1.4 Field of study	Informatics
1.5 Study cycle	Masters
1.6 Study programme / Qualification	Cybersecurity / Specialist in security-focused procedures and tools for information systems

2. Information about the subject/discipline

2.1 Name	Cryptography and information security						
2.2 Course coordinator							
2.3 Seminar coordinator							
2.4 Year of study	1	2.5 Semester	1	2.6 Type of assessment	E	2.7 Type of discipline	DO

3. Total estimated time (hours of teaching per semester)

3.1 Number of hours per week	3	3.2 course	2	3.3 seminars/labs	1
3.4 Total hours in the curriculum	42	3.5 course	28	3.6 seminars/labs	14
Distribution of time:					hours
Study based on Instructions, course materials, bibliography and notes					35
Additional documentation library, specialized electronic platforms / field					30
Training seminars / laboratories, homework, essays, portfolios and essays					30
Tutoring					7
Examinations					6
Other activities					
3.7 Total hours of individual study	108				
3.8 Total hours per semester	150				
3.9 Number of credits	6				

4. Prerequisites (where applicable)

4.1 of curriculum	Operating Systems, Programming, Security and Cryptography, Computer Networks
4.2 of skills	Basic knowledge of computer usage

5. Conditions (where applicable)

5.1 for the course	Classroom properly equipped with: whiteboard, laptop/projector, computers, network, internet connection,
---------------------------	--

	appropriate software. Means for organizing online course activities: Google Classroom, Meet+Chat/Microsoft Teams, PowerPoint, Forms, virtual whiteboard, other specific software components for online activities
5.2 for the seminar	Laboratory classroom properly equipped with: whiteboard, laptop/projector, computers, network, internet connection, appropriate software. Means for organizing online course activities: Google Classroom, Meet+Chat/Microsoft Teams, PowerPoint, Forms, virtual whiteboard, other specific software components for online activities

6. Discipline objectives – learning outcomes

Knowledge	Understanding the mathematical foundations of cryptography and cryptographic analysis Knowledge and ability to apply methods of encryption and decryption Ability to apply hash functions and use digital certificates Security norms and prevention methods
Skills	Understanding the need to keep up with the latest developments and technologies in data transmission, storage, and protection Understanding the need for secure communication in everyday life Recognition of security threats and the need to implement measures to prevent and counter them Ability to decide on the opportunity to use a platform and a programming language in implementing a complex application Knowledge and acquisition of advanced skills in using the main security concepts - hash functions, key sharing protocols, data encryption/decryption algorithms, digital signatures and certificates, public key infrastructure, data protection principles, as well as secure communication
Responsibility and autonomy	A good understanding of the mathematical foundations of cryptography and cryptographic analysis Knowledge and application of the main methods of encrypting and decrypting messages as well as key sharing methods Understanding the nature of security threats Ability to recognize and prevent security threats Ability to implement secure communication methods

7. Contents

7.1 Course	Teaching methods	Comments
Lecture 1: Case study: Breaking down modern depictions of	Video analysis, discussions and debates, modelling, projects, organized team-work	1 week – 2 hours

Information Security examples and hacking breaches		
Lecture 2: Good practices for securing data. Definition of security: IND-CPA. History of cryptography	Exercises, discussions and debates, modelling, projects, organized team-work	1 week – 2 hours
Lecture 3: Trapdoor functions. RSA, trapdoor permutations and another public-key cryptosystem. QRA, Goldwasser-Micali and Homomorphism.	Exercises, discussions and debates, modelling, projects, organized team-work	1 week – 2 hours
Lecture 4: Digital Signatures: Definition. Lamport's One-time Signature Scheme.	Exercises, discussions and debates, modelling, projects, organized team-work	1 week – 2 hours
Lecture 5: Collision-resistant hash functions. Many-time, stateful, signature schemes. Naor-Yung construction: stateless EUF-CMA-secure signature schemes.	Exercises, discussions and debates, modelling, projects, organized team-work	1 week – 2 hours
Lecture 6: Instantiation of collision-resistant hash functions from discrete log. Direct construction of digital signatures from RSA. The hash-and-sign paradigm and the random oracle heuristic. Variants of digital signatures.	Exercises, discussions and debates, modelling, projects, organized team-work	1 week – 2 hours
Lecture 7: Zero knowledge I, definitions and examples. Zero Knowledge Proofs for all of NP.	Exercises, discussions and debates, modelling, projects, organized team-work	1 week – 2 hours
Lecture 8: Succinct (Zero Knowledge) Argument Systems.	Exercises, discussions and debates, modelling, projects, organized team-work	1 week – 2 hours

Tools: Merkle Trees, Probabilistically Checkable Proofs . Kilian's Protocol.		
Lecture 9: Lattices, Learning with Errors (LWE). LWE-based Cryptography: Secret-key and Public-key Encryption, Collision-Resistant Hashing. Fully Homomorphic Encryption. A Construction of FHE from the LWE assumption.	Exercises, discussions and debates, modelling, projects, organized team-work	1 week – 2 hours
Lecture 10: Fully Homomorphic Encryption continued: The Bootstrapping Theorem, and Circular Security. Open Problems in FHE Research.	Exercises, discussions and debates, modelling, projects, organized team-work	1 week – 2 hours
Lecture 11: Oblivious Transfer. Private Information Retrieval.	Exercises, discussions and debates, modelling, projects, organized team-work	1 week – 2 hours
Lecture 12: Secure Two-Party Computation. The Goldreich-Micali-Wigderson Protocol.	Exercises, discussions and debates, modelling, projects, organized team-work	1 week – 2 hours
Lecture 13: Secret-Sharing. Secure Multiparty Computation.	Exercises, discussions and debates, modelling, projects, organized team-work	1 week – 2 hours
Lecture 14: Program Obfuscation and Applications.	Exercises, discussions and debates, modelling, projects, organized team-work	1 week – 2 hours
Bibliography:		
Lecture 2:		
<ul style="list-style-type: none"> • Lecture Notes on the Complexity of Some Problems in Number Theory by Dana Angluin. • Probabilistic Encryption by Shafi Goldwasser and Silvio Micali. 		

- [A Method for Obtaining Digital Signatures and Public-Key Cryptosystems](#) by R.L. Rivest, A. Shamir, and L. Adleman
- [Generating Random Factored Numbers, Easily](#) by Adam Kalai.
- [New Directions in Cryptography](#) by Whitefield Diffie and Martin E. Hellman.
- [Secure Communications Over Insecure Channels](#) by Ralph C. Merkle
- [The Growth of Cryptography](#) by Ronald L. Rivest, at the 2011 Killian Lecture.
- DES specification - FIPS 46-3 - csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
- AES specification - FIPS 197 - csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Lecture 3:

- [Probabilistic Encryption by Shafi Goldwasser and Silvio Micali.](#)
- [A Minimalist Proof of the Law of Quadratic Reciprocity by Bogdan Veklych.](#)

Lecture 4:

- [Goldwasser-Micali-Rivest Signature Scheme](#) by Shafi Goldwasser, Silvio Micali, and Ron Rivest.
- [Two Remarks Concerning the Goldwasser-Micali-Rivest Signature Scheme](#) by Oded Goldreich
- [Universal One-way Hash Functions and their Cryptographic Applications](#) by Moni Naor and Moti Yung.

Lecture 5:

- [SPHINCS: Practical stateless hash-based signatures.](#) by Bernstein et al. (a modern version of the signature scheme from this lecture.)
- SHA-1 specification - FIPS 180-2 - csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf
- [Post-Quantum Cryptography](#) by NIST. See also: [SPHINCS+](#)

Lecture 6:

- [One-Way Functions are Necessary and Sufficient for Secure Signatures](#) by John Rompel.
- DSS specification - FIPS 186-4 - <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>

Lecture 7:

- [The Knowledge Complexity of Interactive Proof Systems](#) by Shafi Goldwasser, Silvio Micali, and Charles Rackoff.

Lecture 8:

- [ZK for NP](#) by Oded Goldreich, Silvio Micali, and Avi Wigderson.

Lecture 9:

- [On Lattices, Learning with Errors, Random Linear Codes, and Cryptography](#) by Oded Regev.
- [Efficient Fully Homomorphic Encryption from \(Standard\) LWE](#) by Zvika Brakerski and Vinod Vaikuntanathan.

- [Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based](#) by Craig Gentry, Amit Sahai and Brent Waters.
- [Hardness of LWE on General Entropic Distributions](#) by Zvika Brakerski and Nico Döttling.
- [Homomorphic Encryption: from Private-Key to Public-Key](#) by Ron Rothblum.

Lecture 10-11:

- [How to Exchange and Generate Secrets](#) by Andrew Chi-Chih Yao
- [Private Information Retrieval](#) by Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan

Lecture 12:

- [Draft of A Chapter on General Protocols](#) from Volume 2 of Foundations of Cryptography, by Oded Goldreich
- [Bar-Ilan Winter School on MPC](#)

Lecture 13:

- [How To Play Any Mental Game](#) by Oded Goldreich, Silvio Micali, and Avi Wigderson
- [Extending Oblivious Transfers Efficiently](#) by Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank
- [Correlated Pseudorandomness and the Complexity of Private Computations](#) by Donald Beaver
- [Simplified VSS and Fast-track Multiparty Computations with Applications to Threshold Cryptography](#) by Rosario Gennaro, Michael O. Rabin, and Tal Rabin
- [Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation](#) by Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson
- [NIST Kick-Starts 'Threshold Cryptography' Development Effort](#)

Lecture 14:

- [On the \(Im\)possibility of Obfuscating programs](#), Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang.
- [How to Use Indistinguishability Obfuscation: Deniable Encryption, and More](#), Amit Sahai and Brent Waters.
- [Indistinguishability Obfuscation from Well-Founded Assumptions](#), Aayush Jain, Huijia Lin and Amit Sahai.

7.2. Seminar	Teaching methods	Comments
<p>1. Cipher text algorithms implementation.</p>	<p>Introduction to the concept of cryptography. Presentation of the evolution of algorithms. Implementation of an application that uses the studied algorithms to transmit information Mini-hackaton type exercises: find the flag/the cipher in a codified message</p>	<p>1 week – 2 hours Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform</p>

<p>2. Public-key encryption. Diffie-Hellman key exchange. Diffie-Hellman/El Gamal encryption. RSA implementation</p>	<p>Defining the asymmetric encryption concept. Discussing the differences between the mechanisms studied in the previous laboratory and those that use private/public key pairs. Implementing a key exchange mechanism Implementing an application capable of securely transmitting keys and encrypted data</p>	<p>1 week – 2 hours Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform</p>
<p>3. Digital Signatures implementation Hash functions implementation</p>	<p>Utilizing the studied concepts to create digital signatures. Case study and in-depth exploration through implementation and research of existing digital signature mechanisms Defining the concepts of hash functions. Implementation of applications that use and validate data through a hashing mechanism. Mini-hackaton type exercises</p>	<p>1 week – 2 hours Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform</p>
<p>4. Merkle's key exchange protocol Merkle Trees implementation</p>	<p>Defining the concept of Merkle trees. Case study and presentation in the form of an article of the concepts that utilize Merkle trees (e.g., Blockchain). Mini-hackaton type exercises: create and validate a merkle tree based hash.</p>	<p>1 week – 2 hours Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform</p>
<p>5. LWE-based Cryptography implementation</p>	<p>Defining the concept of homomorphic encryption. Defining the concept of post-quantum encryption. Case study on Learning With Errors (LWE)</p>	<p>1 week – 2 hours Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform</p>
<p>6. Oblivious Transfer. Private Information Retrieval.</p>	<p>Defining the concept of Oblivious Transfer/Private Information Retrieval. Case study/in-depth exploration through the implementation of an application utilizing the studied concept.</p>	<p>1 week – 2 hours Laboratory notes, laboratory topic information available through specific</p>

		platforms at e-uvt.ro, communication through the Google Classroom platform
7. Program Obfuscation	Studying the obfuscation mechanisms/paradigms. Implementing an application for detecting obfuscated data/Implementing an encryption + obfuscation application. Mini-hackaton type exercises	1 week – 2 hours Laboratory notes, laboratory topic information available through specific platforms at e-uvt.ro, communication through the Google Classroom platform

Bibliography:

- 🔗 [New Directions in Cryptography](#) by Whitefield Diffie and Martin E. Hellman.
- 🔗 [Secure Communications Over Insecure Channels](#) by Ralph C. Merkle
- 🔗 [Universal One-way Hash Functions and their Cryptographic Applications](#) by Moni Naor and Moti Yung.
- 🔗 [SPHINCS: Practical stateless hash-based signatures](#), by Bernstein et al. (a modern version of the signature scheme from this lecture.)
- 🔗 [One-Way Functions are Necessary and Sufficient for Secure Signatures](#) by John Rompel.
- 🔗 Real-World Cryptography, David Wong
- 🔗 [Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based](#) by Craig Gentry, Amit Sahai and Brent Waters.
- 🔗 [Hardness of LWE on General Entropic Distributions](#) by Zvika Brakerski and Nico Döttling.
- 🔗 [Homomorphic Encryption: from Private-Key to Public-Key](#) by Ron Rothblum.
- 🔗 [How to Exchange and Generate Secrets](#) by Andrew Chi-Chih Yao
- 🔗 [On the \(Im\)possibility of Obfuscating programs](#), Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang.
- 🔗 [How to Use Indistinguishability Obfuscation: Deniable Encryption, and More](#), Amit Sahai and Brent Waters.
- 🔗 [Indistinguishability Obfuscation from Well-Founded Assumptions](#), Aayush Jain, Huijia Lin and Amit Sahai.
- 🔗 DES specification - FIPS 46-3 - csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
- 🔗 AES specification - FIPS 197 - csrc.nist.gov/publications/fips/fips197/fips-197.pdf
- 🔗 SHA-1 specification - FIPS 180-2 - csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf
- 🔗 DSS specification - FIPS 186-4 - <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>

8. Corroboration of the course contents with the epistemic expectations of the community representative, professional associations and representative employers of the programme itself

Class contents correspond to the curricula of other universities, from inside the country or from the European Union. The practical contents (laboratory works) correspond to the local labour market requirements.

9. Evaluation

Type of activity	9.1 Evaluation criteria	9.2 Evaluation methods	9.3 Percentage of the final mark
9.4 Course	The evaluation takes into account the following categories of knowledge <ul style="list-style-type: none"> • general knowledge, evaluated through an implemented project based on state-of-the-art approaches linked to discussed topics. • detailed knowledge, evaluated through implementation/experimental results based on own/state-of-the-art approaches. • use of algorithms, evaluated through a test consisting of a set of problems based on the algorithms presented/implemented in class 	Written/presentation examination; active participation in class activities.	60 %
9.5 Seminar	Mandatory laboratory assignments	Evaluation of assignments, additional activities	40 %
9.6 Minimum performance standards			
<p>To obtain a passing grade of 5 for the entire subject, it is necessary to obtain a score higher than 60% for the general knowledge, as well as to demonstrate a minimum level of understanding and application of some of the algorithms presented in the course (at least 40%). The minimum passing grade for both the course and seminar must be at least 5.</p> <p>To obtain a grade of 10, it is necessary to obtain a score higher than 95% for both general knowledge and detailed knowledge, as well as a good understanding of the presented algorithms.</p>			

Date of submission:

Titular of the course:

Date of approval in department:

Seminary titular:

HEAD OF THE DEPARTMENT:

SYLLABUS

1. Information about the study programme

1.1 Institution of higher education	West University of Timișoara
1.2 Faculty	Mathematics and Informatics
1.3 Department of	Informatics
1.4 Field of study	Computer Science
1.5 Study cycle	Bachelor
1.6 Study programme / Qualification	Computer Science Database administration / <i>Administrator baze de date - 252101</i> ; Computer network administration / <i>Administrator de retea de calculatoare - 252301</i> ; Analyst / <i>Analist - 251201</i> ; Research assistant in computer science / <i>Asistent de cercetare în informatica - 214918</i> ; Teacher in secondary schools / <i>Profesor în învățământul gimnazial - 233002</i> ; Programmer / <i>Programator - 251202</i> ; Software systems designers / <i>Proiectant sisteme informatice - 251101</i>

2. Information about the subject/discipline

2.1 Name	Operating Systems I						
2.2 Course coordinator							
2.3 Seminar coordinator							
2.4 Year of study	2	2.5 Semester	1	2.6 Type of assessment	E	2.7 Type of discipline	M

3. Total estimated time (hours of teaching per semester)

3.1 Number of hours per week	4	3.2 course	2	3.3 seminars/labs	2
3.4 Total hours in the curriculum	56	3.5 course	28	3.6 seminars/labs	28
Distribution of time:					hours
Study based on Instructions, course materials, bibliography and notes					42
Additional documentation library, specialized electronic platforms / field					28
Training seminars / laboratories, homework, essays, portfolios and essays					28
Tutoring					2
Examinations					5
Other activities					-
3.7 Total hours of individual study	112				
3.8 Total hours per semester	168				
3.9 Number of credits	5				

4. Prerequisites (where applicable)

4.1 of curriculum	Computer Architecture, Programming I, Programming II
--------------------------	--

4.2 of skills	C1. Programarea în limbaje de nivel înalt C2. Dezvoltarea și întreținerea aplicațiilor informatice. C4. Utilizarea bazelor teoretice ale informaticii.
----------------------	--

5. Conditions (where applicable)

5.1 for the course	Access to the Internet, with a Web-compatible browser.
5.2 for the seminar	Access to the Internet, with a laptop or computer capable of running the Linux and Windows operating systems.

6. Discipline objectives – learning outcomes

Knowledge	<ul style="list-style-type: none"> • Developing skills for using operating systems • The ability to understand and use the basic concepts of operating systems • The ability to solve problems in the context of using operating systems
Skills	<ul style="list-style-type: none"> • Using methodologies, specification mechanisms, and development environments for creating software applications • Using appropriate criteria and methods for evaluating software applications • Developing and maintaining software applications to solve real-world problems of medium complexity
Responsibility and autonomy	<ul style="list-style-type: none"> • Using methodologies and environments for designing and managing computing systems, databases, and computer networks for specific problems • Developing projects for computing systems, databases, and computer networks

7. Contents

7.1 Course	Teaching methods	Comments
<p>Introduction. History. Generations of Operating Systems. The evolution of basic concepts; The Computing System: the processor, the memory, I/O devices, system bus; Structure of (modern) computing systems: monolithic, layered, virtual machines, client-server.</p> <p>Fundamentals. Basic notions: processes, deadlock, memory management, I/O devices, security; System calls: process management, file and directory management, other system calls. Hardware components of a computing system; Mapping of hardware components on basic operating systems concepts.</p>	Exercise, discussions and debate, modeling, project work, organized group work.	2 weeks – 4 hours

<p>Processes and threads. Process description and process control. Process model; Creation and termination of processes; Process states. Hierarchies of processes; Information about processes, cooperating processes, process scheduling. Threads; Threads description and control. Usage of threads; Threads implementation. Threads in user space, threads in kernel space, pop-up threads, mixed approach; Typical problems in thread usage.</p>	<p>Exercise, discussions and debate, modeling, project work, organized group work.</p>	<p>2 weeks – 4 hours</p>
---	--	---------------------------------

<p>Inter-process communication (IPC). Basis of IPC communication: race conditions, critical regions, mutual exclusion, busy waiting.</p> <p>Mutual exclusion. Solutions for busy waiting: interrupt deactivation, strict alternation, TSL instruction, lock variables etc.; Synchronizing execution: sleep/wakeup, semaphores, mutex, monitores, barriers, message passing.</p> <p>Classical problems of inter-process communication. The dining philosophers; Readers and writers; Barbershop; Consumer-producer. Implications of these problems in modern operating systems.</p>	<p>Exercise, discussions and debate, modeling, project work, organized group work.</p>	<p>2 weeks – 4 hours</p>
<p>Process scheduling. Scheduling. General information. Scheduling in different operating systems. Goals of scheduling; Scheduling in batch-processing systems; Scheduling in interactive systems; Threads scheduling.</p>	<p>Exercise, discussions and debate, modeling, project work, organized group work.</p>	<p>2 weeks – 4 hours</p>
<p>Deadlocks. Preemptive and non-preemptive resources, resource acquisition, deadlock conditions, deadlock modeling; Ostrich algorithm; Detection, avoidance, prevention of deadlocks. Algorithms for deadlock detection, avoidance, prevention; Banker’s algorithm</p>	<p>Exercise, discussions and debate, modeling, project work, organized group work.</p>	<p>2 weeks – 4 hours</p>
<p>Memory management. Basic notions. Monoprogramming and multiprogramming; Memory relocation and memory protection; Swapping. Memory management (swapping based); Virtual memory. Pagination, page tables.</p>	<p>Exercise, discussions and debate, modeling, project work, organized group work.</p>	<p>2 weeks – 4 hours</p>
<p>Memory management. Page replacement algorithms; Modeling page replacement algorithms; Requirements for the implementation of memory management; Segmentation.</p>	<p>Exercise, discussions and debate, modeling, project work, organized group work.</p>	<p>2 weeks – 4 hours</p>
<p>Bibliography:</p> <ol style="list-style-type: none"> 1. A. S. Tanenbaum, “Modern Operating Systems”, 2nd edition (cel putin), Prentice Hall International 2. A. Silberschatz, P.B. Galvin, “Operating Systems Concepts”, 4th edition (cel putin), Addison Wesley 3. W. Stallings, “Operating Systems”, 4th edition (cel putin), Prentice-Hall 4. M. Bach, “The Design of the UNIX Operating System”, Prentice-Hall, 1981. 5. F. Fortiș, “Sisteme de operare. Suport de curs”, Eubeea, 2005. 6. F. Fortis, V. Negru, C. Sandru, “Inițiere in UNIX”, Eubeea, 2001. 7. C. Pungilă, website, http://web.info.uvt.ro/~cpungila 		
<p>7.2. Seminar</p>	<p>Teaching methods</p>	<p>Comments</p>

Connecting to the system, working at system console/terminal, using the graphical interface. Typical compilation commands of a C program in Linux.	The exercise, discussions and debate, modeling, project work, organized group work.	2 weeks – 4 hours
Tools in a Linux environment: the text editor, the make utility, manual pages. Syscalls for file and directory management. Practical examples.	The exercise, discussions and debate, modeling, project work, organized group work.	2 weeks – 4 hours
Processes. Syscalls for process management in Linux. Practical examples.	The exercise, discussions and debate, modeling, project work, organized group work.	2 weeks – 4 hours
Pipes. Syscalls for creating and managing pipes in Linux. Redirection of input/output. Practical examples.	The exercise, discussions and debate, modeling, project work, organized group work.	2 weeks – 4 hours
Inter-process communication (IPC). Signals. Syscalls for signal management and handling. Practical examples.	The exercise, discussions and debate, modeling, project work, organized group work.	2 weeks – 4 hours
Threads. Syscalls for managing and creating threads in Linux. Common thread issues. Practical examples.	The exercise, discussions and debate, modeling, project work, organized group work.	2 weeks – 4 hours
Thread synchronization. Race conditions. Mutual exclusion. Shared memory. Syscalls for thread synchronization and shared memory management.	The exercise, discussions and debate, modeling, project work, organized group work.	2 weeks – 4 hours
Bibliography:		
8. A. S. Tanenbaum, "Modern Operating Systems", 2nd edition (cel putin), Prentice Hall International		
9. A. Silberschatz, P.B. Galvin, "Operating Systems Concepts", 4th edition (cel putin), Addison Wesley		
10. W. Stallings, "Operating Systems", 4th edition (cel putin), Prentice-Hall		
11. M. Bach, "The Design of the UNIX Operating System", Prentice-Hall, 1981.		
12. F. Fortiș, "Sisteme de operare. Suport de curs", Eubeea, 2005.		
13. F. Fortis, V. Negru, C. Sandru, "Initiere in UNIX", Eubeea, 2001.		
14. C. Pungilă, website, http://web.info.uvt.ro/~cpungila		

8. Corroboration of the course contents with the epistemic expectations of the community representative, professional associations and representative employers of the programme itself

The course content aligns with the curriculum from other university centers, both in the country and the European Union. The practical content (laboratory work) meets the requirements of the local job market.

9. Evaluation

Type of activity	9.1 Evaluation criteria	9.2 Evaluation methods	9.3 Percentage of the final mark
------------------	-------------------------	------------------------	----------------------------------

9.4 Course	The evaluation takes into account the following categories of knowledge: <ul style="list-style-type: none">• General knowledge,	A. Written examination;	A. 40% B. 10%
-------------------	---	-------------------------	------------------

	<p>assessed through a test containing multiple-choice questions or basic definitions</p> <ul style="list-style-type: none"> • Detailed knowledge, assessed through a test focused on the key concepts taught • The use of algorithms, assessed through a test containing a set of problems based on the algorithms presented in the course. 	<p>B. Active participation in course activities.</p>	
<p>9.5 Seminar</p>	<p>The evaluation considers the following categories of knowledge:</p> <ul style="list-style-type: none"> • General knowledge, ability to navigate and manage UNIX-based systems • General low-level API calls for creating processes and threads • General API calls for inter-process communication through pipes and signals • General API calls for multi-thread programming and thread synchronization • The use of algorithms, assessed through a test containing a set of problems based on the algorithms presented during the laboratories. 	<p>A. Evaluation of laboratory activities;</p> <p>B. Active participation in laboratory activities;</p> <p>C. Written examination at the end of the semester.</p>	<p>A. 10%</p> <p>B. 05%</p> <p>C. 35%</p>
<p>9.6 Minimum performance standards</p>			

Written examination:

- For a grade of 5, it is necessary to achieve a superior score (at least 60%) in general knowledge, as well as demonstrating a minimum level of understanding and application of some of the algorithms presented in the course (at least 40%).
- For a grade of 10, it is necessary to achieve a superior score (at least 75%) in general and detailed knowledge, as well as a good understanding of the algorithms presented.

Practical tests and laboratory activity:

For a grade of 5, it is necessary to achieve a superior level (at least 60%) in general knowledge, as well as a minimum level of understanding and application of the detailed knowledge previously presented.

For a grade of 10, it is necessary to demonstrate a superior level (at least 80%) in the advanced knowledge specified earlier.

Date of submission:

Titular of the course:

Signature:

Date of approval in department:

Seminary titular:

Signature:

HEAD OF THE DEPARTMENT:

FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea de Vest din Timișoara
1.2 Facultatea / Departamentul	Matematică și Informatică
1.3 Departamentul	Informatică
1.4 Domeniul de studii	Informatică
1.5 Ciclul de studii	licență
1.6 Programul de studii / Calificarea	Informatică / <i>Administrator baze de date - 252101; Administrator de rețea de calculatoare - 252301; Analist - 251201; Asistent de cercetare în informatica - 214918; Asistent de cercetare în matematica-informatica - 212024; Profesor în învățământul gimnazial - 233002; Programator - 251202; Proiectant sisteme informatice - 251101</i>

2. Date despre disciplină

2.1 Denumirea disciplinei	Proiect Colectiv						
2.2 Titularul activităților de curs							
2.3 Titularul activităților de seminar							
2.4 Anul de studiu	2	2.5 Semestrul	2	2.6 Tipul de evaluare	C	2.7 Regimul disciplinei	O

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1 Număr de ore pe săptămână	1	din care: 3.2 curs		3.3 seminar/laborator	1
3.4 Total ore din planul de învățământ	14	din care: 3.5 curs		3.6 seminar/laborator	14
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie și notițe					10
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate / pe teren					10
Pregătire seminare / laboratoare, teme, referate, portofolii și eseuri					20
Tutorat					10
Examinări					6
Alte activități					5
3.7 Total ore studiu individual	61				
3.8 Total ore pe semestru	75				
3.9 Numărul de credite	3				

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	<ul style="list-style-type: none"> POO, Inginerie software, Baze de date
4.2 de competențe	<ul style="list-style-type: none"> Programarea în limbaje de nivel înalt

5. Condiții (acolo unde este cazul)

5.1 de desfășurare a cursului	<ul style="list-style-type: none"> Nu e cazul
5.2 de desfășurare a seminarului / laboratorului	<ul style="list-style-type: none"> Blended Learning Echipamente de calcul de tip PC/laptop cu componente audio/video funcționale, acces la internet, echipamente video funcționale Activitățile online se vor realiza pe Moodle: https://elearning.e-uvt.ro/course/view.php?id=101526

6. Obiectivele disciplinei - rezultate așteptate ale învățării la formarea cărora contribuie parcurgerea și promovarea disciplinei

Cunoștințe	<ul style="list-style-type: none"> programarea în limbaje de nivel înalt; analiza și parcurgerea etapelor de realizare a proiectelor informatice, dezvoltarea și întreținerea aplicațiilor informatice.
Abilități	<ul style="list-style-type: none"> munca în echipă în scopul realizării proiectelor informatice, utilizarea unui instrument software în realizarea unui produs/serviciu original, rezolvarea problemelor în mod creativ/inovativ, comunicare eficientă scris și oral între membrii echipei și cu clienții/utilizatorii.
Responsabilitate și autonomie	<ul style="list-style-type: none"> organizarea/managementul activității, capacitate de reflexie pe baza experienței pe parcursul realizării proiectului, autoformare prin procesul de documentare și realizare a proiectului, urmărirea și realizarea obiectivelor stabilite.

7. Conținuturi

7.1 Curs	Metode de predare	Observații
7.2 Seminar / laborator	Metode de predare	Observații
1. Metode, tehnici și instrumente utilizate în managementul proiectelor	Expunere și comunicare	Formarea echipelor de proiect
2. Analiza temelor propuse pentru Proiectul Colectiv	Învățarea prin descoperire	Comunicare online
3. Validarea temelor propuse pe baza scopului, obiectivelor și a indicatorilor de performanță ai proiectului propus	Studiul de caz Metoda proiectelor	Comunicare online
4. Verificarea și validarea etapelor de realizare a Proiectului Colectiv	Studiu de caz Comunicarea Metoda proiectelor	Comunicare online
5. Elaborarea, prezentarea și validarea livrabilelor realizate în Proiectul Colectiv	Învățarea prin descoperire Studiul de caz	Comunicare online
6. Analiza statusului proiectului și revederea versiunii beta a Proiectului Colectiv	Metoda proiectelor	Comunicare online
7. Prezentarea și evaluarea produsului/serviciului final al Proiectului Colectiv	Studiul de caz	Comunicare online
Bibliografie :		
1. Ian Sommerville, "Software Engineering" Eighth Edition, Addison-Wesley, 2007		
2. Heagney, Joseph, Fundamentals of project management —4th ed, American Management Association, NY, 2012		
3. A. Dennis, B. H. Wixom, R. M. Roth, "System Analysis and Design", Fifth Edition, John Wiley &		

Sons, Inc., 2012

4. http://www.opentextbooks.org.hk/system/files/export/15/15694/pdf/Project_Management_15694.pdf
5. http://www.saigontech.edu.vn/faculty/huyng/SAD/Systems_Analysis_Design_UML_5th
6. <https://www.studytonight.com/dbms/database-normalization.php>
7. <https://www.cmu.edu/teaching/index.html>
8. https://en.wikipedia.org/wiki/Project_management
9. <https://www.projectmanager.com/training/what-are-project-deliverables>

8. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

Conținutul disciplinei vizează pregătirea practică a studenților în vederea integrării pe piața muncii. Activitățile sunt realizate în parteneriat cu angajatori reprezentativi din domeniul IT: Nokia, IBM, Continental, Microsoft, Hella, etc.

9. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
9.4 Curs	-	-	-
9.5 Seminar / laborator	Documentație proiect Aplicație Ansamblu proiect Conținut Prezentare proiect Răspunsuri la întrebări la susținere	Proiect Proiect Evaluare formativă Proiect Evaluare sumativă Evaluare sumativă	1/5 1/5 1/5 1/5 1/10 1/10
Punctajul individual al membrilor echipei se va repartiza în cadrul echipei de către membrii echipei.			
10.6 Standard minim de performanță			
<ol style="list-style-type: none"> 1. Validarea temei de proiect: proiectul va conține baze de date, va utiliza minim un limbaj de programare de nivel înalt și va dezvolta minimum trei funcționalități. 2. Realizarea <i>etapei de analiză proiect completă</i>, cu documentația aferentă. 3. Etapele de proiectare și implementare vor fi parcurse <i>până la realizarea unei versiuni de test/beta</i> a aplicației propuse în tema de proiect. 4. Disciplina poate fi promovată dacă sunt realizate cumulativ cerințele 1,2,3. 			

Data completării

Titular de disciplină

Data avizării în departament

Director de departament

FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea de Vest din Timișoara
1.2 Facultatea / Departamentul	Matematică și Informatică
1.3 Departamentul	Informatică
1.4 Domeniul de studii	Informatică
1.5 Ciclul de studii	licență
1.6 Programul de studii / Calificarea	Informatică / <i>Administrator baze de date - 252101; Administrator de rețea de calculatoare - 252301; Analist - 251201; Asistent de cercetare în informatica - 214918; Asistent de cercetare în matematica-informatica - 212024; Profesor în învățământul gimnazial - 233002; Programator - 251202; Proiectant sisteme informatice - 251101</i>

2. Date despre disciplină

2.1 Denumirea disciplinei	Securitate și Criptografie						
2.2 Titularul activităților de curs							
2.3 Titularul activităților de seminar							
2.4 Anul de studiu	3	2.5 Semestrul	2	2.6 Tipul de evaluare	E	2.7 Regimul disciplinei	DO P

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1 Număr de ore pe săptămână	4	din care: 3.2 curs	2	3.3 seminar/laborator	2
3.4 Total ore din planul de învățământ	4	din care: 3.5 curs	2	3.6 seminar/laborator	24
	8		4		
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie și notițe					24
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate / pe teren					24
Pregătire seminare / laboratoare, teme, referate, portofolii și eseuri					24
Tutoriat					3
Examinări					2
Alte activități					
3.7 Total ore studiu individual					77
3.8 Total ore pe semestru					125
3.9 Numărul de credite					5

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	SO, Programare
-------------------	----------------

4.2 de competențe	Programare în limbaje de nivel înalt
-------------------	--------------------------------------

5. Condiții (acolo unde este cazul)

5.1 de desfășurare a cursului	Sală de curs cu tablă și proiector.
5.2 de desfășurare a seminarului / laboratorului	Sală de laborator cu tablă, proiector și calculatoare.

6. Obiectivele disciplinei - rezultate așteptate ale învățării la formarea cărora contribuie parcurgerea și promovarea disciplinei

Cunoștințe	Înșușirea conceptelor de bază în securitatea rețelelor și criptografie Înșușirea conceptelor și problematicii securității rețelelor de calculatoare prin utilizarea algoritmilor de criptare
Abilități	Abilitatea de proiectare a algoritmilor de criptare în vederea realizării unei rețele securizate Abilitatea de a administra rețelele de calculatoare în condiții de securitate ridicată
Responsabilitate și autonomie	Aplicarea regulilor de muncă riguroasă și eficientă, manifestarea unor atitudini responsabile față de domeniul științific și didactic, pentru valorificarea optimă și creativă a propriului potențial în situații specifice, cu respectarea principiilor și a normelor de etică profesională Desfășurarea eficientă și eficace a activităților organizate în echipă Utilizarea eficientă a surselor informaționale și a resurselor de comunicare și formare profesională asistată

7. Conținuturi

7.1 Curs	Metode de predare	Observații
C1. Concepte de securitate și criptografie.	Expunere interactivă. Prelegere însoțită de materiale în format electronic (PDF)	Temele disponibile prin platforme specifice e-uvt.ro, comunicare prin platforma Google Classroom
C2. Clasificarea metodelor de criptare. Criptografie clasică și tendințe actuale în criptografie și analiza criptografică	Prelegere însoțită de materiale în format electronic (PDF). Expunere interactivă.	idem
C3-C4 Criptarea convențională clasică. Modelul criptării convenționale Algoritmi de cifrare clasici (Codul lui Caesar, Roata alfabetică, Tabele Viginere, Tabela Porta, Codificări matrice, Codificări Bifid, Codificări cu transpoziție, Codul Playfair, Codul Hill)	Prelegere însoțită de materiale în format electronic (PDF). Expunere interactivă.	idem
C6-C7. Algoritmi moderni de criptare. Principiile codurilor bloc. Structura codului Feistel. Algoritmii: DES, Triplu DES, IDEA, RC5, AES	Prelegere însoțită de materiale în format electronic (PDF). Expunere interactivă.	idem

C8. Criptarea cu chei publice. Algoritmul RSA. Algoritmul Diffie-Hellman	Prelegere însoțită de materiale în format electronic (PDF)	idem
C9. Funcții hash, semnături digitale.	Prelegere însoțită de materiale în format electronic (PDF)	idem
C10. Administrarea cheilor	Prelegere însoțită de materiale în format electronic (PDF). Expunere interactivă.	idem
C11. Tehnici de atac și apărare în era internetului.	Prelegere însoțită de materiale în format electronic (PDF). Expunere interactivă.	idem
C12. Criptarea cuantică	Prelegere însoțită de materiale în format electronic (PDF).	idem
<p>Bibliografie:</p> <ol style="list-style-type: none"> 1. Understanding Cryptography: A Textbook for Students and Practitioners by Christof Paar and Jan Pelz 2. Nicolae Constantinescu. Criptografie. Ed. Academiei Române, 2009 3. Lars Klander - Anti Hacker. Ghidul securității rețelelor de calculatoare - Editura All Educational, 1998 4. Harold F. Tipton, Micki Krause – Information Security Management Handbook, Auerbach Publications, CRC Press LLC, 2000 5. Jonathan Katz and Yehuda Lindell, <i>Introduction to Modern Cryptography (2nd edition)</i>, (http://www.cs.umd.edu/~jkatz/imc.html). 6. Jonathan Knudsen - Java Cryptography, Editura O'Reilly, 1998 <p>A. Menezes, P. Van Oorschot, S. Vanstone, <i>Handbook of Applied Cryptography</i> (https://cacr.uwaterloo.ca/hac/)</p>		
7.2 Seminar / laborator	Metode de predare	Observații
1-2. Implementarea de algoritmi de criptare clasici	Expunere. Exemplificare interactivă.	Studentii vor lucra individual pentru realizarea exemplurilor de laborator. Temele primite la finalul laboratorului vor fi prezentate în cadrul laboratorului imediat următor și vor fi încărcate la Google Classroom. Temele vor fi disponibile prin platforme specifice e-uvt.ro, iar comunicarea se va face prin platforma Google Classroom
3-4. Implementarea algoritmilor de criptare/decriptare de tip cifruri de substituție polialfabetice: Cifrul lui Vigenere, Cifrul lui Trithemius	Expunere. Exemplificare interactivă.	idem

5-6. DES/AES	Expunere. Exemplificare interactivă.	idem
7. Algoritmi hash	Expunere. Exemplificare interactivă.	idem
8. Exemple de implementări pentru algoritmi cu cheie publică. Algoritmul RSA	Expunere. Exemplificare interactivă.	idem
9. Criptare prin curbe eliptice	Expunere. Exemplificare interactivă.	idem
10. Semnătura și certificarea digitală	Expunere. Exemplificare interactivă.	idem
11-12. Prezentare proiect.	Expunere.	idem
Bibliografie ☒ Jonathan Knudsen - Java Cryptography, Editura O'Reilly, 1998 ☒ DES specification - FIPS 46-3 - csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf ☒ AES specification - FIPS 197 - csrc.nist.gov/publications/fips/fips197/fips-197.pdf ☒ SHA-1 specification - FIPS 180-2 - csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf ☒ DSS specification - FIPS 186-4 - https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf		

8. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

Dezvoltarea abilităților de exploatare a rețelelor de calculatoare pentru potențiali utilizatori. Piața muncii locală, națională sau europeană este în permanentă căutare de absolvenți cu bune cunoștințe în proiectarea unor rețele sigure

9. Evaluare

Tip activitate	9.1 Criterii de evaluare	9.2 Metode de evaluare	9.3 Pondere din nota finală
9.4 Curs	Lucrare scrisă – test grilă și descriptivă- la care se evaluează cunoștințele teoretice dobândite din tematica cursului și a laboratorului. <i>Cerinte minime pentru nota 5: Cunoașterea elementelor fundamentale de teorie.</i> Cerinte pentru nota 10: Cunoașterea tuturor elementelor de teorie predate la curs și la laborator. Realizarea tuturor temelor de laborator.	Examen scris	40%
	Activitate laborator: întocmirea unui proiect	Probă practică pe calculator – prezentarea proiectului	40%
9.5 Seminar / laborator	Temele de laborator obligatorii (algoritmi de criptare/decriptare,criptanaliza)		20%

9.6 Standard minim de performanță
Obținerea notei minime 5(cinci) atât la evaluarea teoretică (curs) cât și la cea practică (laborator)

Data completării

Titular de disciplină

Data avizării în departament

Director de departament

SALARIILE DE ÎNCADRARE

aferente posturilor didactice și de cercetare din învățământul superior, scoase la concurs în anul universitar 2024-2025

Salarizarea candidaților desemnați câștigători pe posturile didactice și de cercetare, scoase la concurs în anul universitar 2024-2025, se va face în conformitate cu prevederile Legii 153/2017, cu completările și modificările ulterioare, încadrarea salarială făcându-se conform grilei de salarizare, astfel:

Nr. crt.	Funcția didactică	Salariul de bază brut la data de 01.09.2024* (lei)
1	Profesor universitar, tranșa 5-10 ani, gradație 2	9.370
2	Conferențiar universitar, tranșa 3-5 ani, gradație 1	7.579
3	Lector universitar, tranșa 3-5 ani, gradație 1	7.246
4	Asistent universitar, tranșa până la 3 ani, gradație 0	6.520
5	Asistent de cercetare științifică, gradație 0	6.035
6	Cercetător științific I, gradație 0	10.222
7	Cercetător științific II, gradație 0	8.120
8	Cercetător științific III, gradație 0	6.550

*nivelul salariului la încadrarea pe post va fi conform Legii 153/2017, cu completările și modificările ulterioare

Direcția Resurse Umane
Dicso Vanessa

Anexa 4 - Statul de funcții 2024 - 2025 al departamentului de Informatică paginile 7-8.

Stat de funcții 2024-2025
Facultatea de Matematica și Informatica
Informatica

Nr. post	Fct.	Tip post	Angajat / Disciplina	Detalii Sp/TipStd./Lb/An	Sem.	Serii/ Grupe	Ore Curs		Ore Sem./L/P		Norma	Alte activ.
							Fiz.	Conv.	Fiz	Conv		
29	Lect	T	IVASCU TODOR								10,5	5,5
29			Programare II	IR1/L/Z/lan1	II	0 / 2	0	0	2	2	2	
29			Programare III	IR2/L/Z/lan2	I	1 / 2	2	2	2	2	4	
29			Sisteme multi-agent - P1	IS1/M/Z/lan1	II	1 / 0	2	2,5	0	0	2,5	
29			Structuri de date avansate	IR2/L/Z/lan2	I	1 / 0	2	2	0	0	2	
30	Lect	T	STEFANIGA SEBASTIAN-AURELIAN								10,31	5,69
30			Robotic process automation	ISR1/En/M/Z/lan1	II	1 / 1	2	3,125	1	0,938	4,06	
30			Robotic process automation - P2	IR3/L/Z/lan3	I	0 / 1	0	0	1	0,5	0,5	
30			Tehnologii web	IR3/L/Z/lan3	I	1 / 0	2	2	0	0	2	
30			Web Design	AI1/En/L/Z/lan1	II	1 / 1	0	0	2	1,25	1,25	
30			Web Design	IE1/En/L/IF/lan1	II	1 / 1	0	0	2	1,25	1,25	
30			Web Design C	(2) +AI1/En/L/Z/lan1+IE1/En/L/IF/lan1	II	1 / 3	1	1,25	0	0	1,25	
31	Lect	TS	REJA MARIO-DANIEL								11,06	4,94
31			Applications, approaches and challenges in cybersecurity in the modern digital era	CS1/En/M/IF/lan1	II	1 / 1	2	3,125	1	0,938	4,06	
31			Rețele de calculatoare	IR2/L/IF/lan2	II	1 / 0	2	2	0	0	2	
31			Sisteme de operare I	IR2/L/IF/lan2	I	0 / 3	0	0	2	3	3	
31			Sisteme de operare II	IR2/L/IF/lan2	II	1 / 1	1	1	2	1	2	
32	Lect	VSC	-vacant CONCURS-								10	6
32			Algorithms and data structures I - C	(2) +AI1/En/L/Z/lan1+IE1/En/L/IF/lan1	I	1 / 0	2	2,5	0	0	2,5	
32			Algorithms and data structures I - S	AI1/En/L/IF/lan1	I	1 / 1	0	0	2	1,25	1,25	
32			Algorithms and data structures I - S	IE1/En/L/IF/lan1	I	1 / 1	0	0	2	1,25	1,25	
32			Algoritmi și structuri de date I	IR1/L/IF/lan1	I	0 / 5	0	0	2	5	5	
33	Lect	VSC	-vacant CONCURS -								10,09	5,91
33			Cryptography and information security - C	(2)+CS1/En/M/IF/lan1	I	1 / 2	2	3,125	0	0	3,13	
33			Operating systems I - L	IE2/En/L/IF/lan2	I	1 / 3	0	0	2	3,75	3,75	

Anexa 4 - Statul de funcții 2024 - 2025 al departamentului de Informatică paginile 7-8.



Rector: Prof. Univ. Dr. Marilen Gabriel PIRTEA

Stat de functii 2024-2025
Facultatea de Matematica si Informatica
Informatica

Nr. post	Fct.	Tip post	Angajat / Disciplina	Detalii Sp/TipStd./Lb/An	Sem.	Serii/ Grupe	Ore Curs		Ore Sem./L/LP		Norma	Alte activ.
							Fiz.	Conv.	Fiz	Conv		
33			Proiect colectiv	IR2/L/IF/an2	II	0 / 3	0	0	1	1,5	1,5	
33			Securitate și criptografie - P1	IR3/L/IF/an3	II	0 / 2	0	0	2	1,714	1,71	
34	Lect	VSC	-vacant CONCURS -								10,23	6,77
34			Introduction to neurotehnologies - P3	IE3/En/L/IF/an3	II	1 / 2	2	2,143	2	2,143	4,29	
34			Introduction to robotics	ISR1/En/M/IF/an1	I	1 / 1	1	1,563	2	1,875	3,44	
34			Software engineering - L	IE2/En/L/IF/an2	II	1 / 2	0	0	2	2,5	2,5	
35	Lect	V	-vacant CONCURS -								10,14	6,86
35			Competențe de antreprenoriat	IR2/L/IF/an2	I	1 / 0	1	1	0	0	1	
35			Intelligent systems and machine learning - P2	IE3/En/L/IF/an3	II	0 / 3	0	0	2	3,214	3,21	
35			Modelare economică - P3	IR3/L/IF/an3	II	1 / 2	2	1,714	2	1,714	3,43	
35			Programming I - L	AI1/En/L/IF/an1	I	0 / 2	0	0	2	2,5	2,5	
36	Lect	VSC	-vacant CONCURS -								10,07	5,93
36			Inteligență artificială	IR2/L/IF/an2	II	0 / 6	0	0	2	6	6	
36			Machine Learning	(4) +CS2/En/M/IF/an2+BD2/En/M/IF/an2+AIDC2/En/M/IF/an2+ISR2/En/M/IF/an2	I	1 / 2	2	3,125	0	0	3,13	
36			Machine Learning - L1	(2) +AIDC2/En/M/IF/an2+CS2/En/M/IF/an2	I	0 / 1	0	0	1	0,938	0,94	
37	Lect	V	VACANT								16,89	0,11
37			Algorithms and data structures II - C	(2) +IE1/En/L/IF/an1+AI1/En/L/ZI/an1	II	1 / 4	2	2,5	0	0	2,5	
37			Calcul paralel - P2	IS1/M/IF/an1	II	1 / 1	2	2,5	1	0,75	3,25	
37			Data mining - C	(4) +ISR1/En/M/IF/an1+BD1/En/M/IF/an1+CS1/En/M/IF/an1+AIDC1/En/M/IF/an1	II	1 / 4	2	3,125	0	0	3,13	
37			Parallel computing - P1 - C	(3) +ISR1/En/M/IF/an1+AIDC1/En/M/IF/an1+BD1/En/M/IF/an1	II	1 / 2	2	3,125	0	0	3,13	
37			Parallel computing - P1 - L1	BD1/En/M/IF/an1	II	1 / 1	0	0	1	0,938	0,94	

Anexa 4 - Statul de funcții 2024 - 2025 al departamentului de Informatică paginile 7-8.

PROCES VERBAL NR. Reg. UVT2025-017565/12.03.2025
al întâlnirii Consiliului Departamentului de Informatică
Din data de 12 martie 2025
= extras =

Încheiat astăzi, 12.03.2025, cu ocazia ședinței extraordinare a Consiliului Departamentului de Informatică din cadrul Facultății de Matematică și Informatică, convocată de dl. Lect. Dr. Cira Cristian, membru al Consiliului Departamentului de Informatică, cu atribuții delegate de Director de Departament Informatică, prin decizia: 175/DRU/2025 , pentru ora 15:45, online, link: <https://meet.google.com/wbs-ahpn-vq>.

1. **Punctul 1** al ordinii de zi l-a constituit **avizarea modificării** modalității de ocupare a postului didactic vacant de **Lector universitar 33**, din statul de funcții al Departamentului de Informatică, pentru anul universitar 2024-2025 din vacant promovare în vacant concurs.

Membrii Consiliului Departamentului de Informatică au avizat favorabil cu unanimitate de voturi punctul 1.

2. **Punctul 2** al ordinii de zi l-a constituit **avizarea referatelor cu privire la necesitatea scoaterii la concurs a posturilor didactice vacante**, prevăzute în statul de funcții al Departamentului de Informatică, anul 2024-2025, aferente semestrului al II-lea:
 - a) Postul de Asistent 66, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.
 - b) Postul de Asistent 68, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.
 - c) Postul de Asistent 69, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.
 - d) Postul de Lector 32, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.
 - e) Postul de Lector 33, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.
 - f) Postul de Lector 34, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.
 - g) Postul de Lector 35, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.

- h) Postul de Lector 36, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.

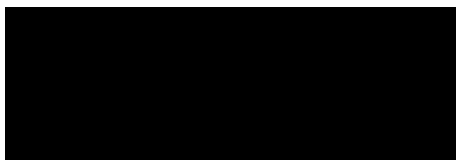
Membrii Consiliului Departamentului de Informatică au avizat favorabil cu unanimitate de voturi următoarele posturi:

- a) Postul de Asistent 66, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.
- b) Postul de Asistent 68, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.
- d) Postul de Lector 32, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.
- e) Postul de Lector 33, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.
- f) Postul de Lector 34, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.
- g) Postul de Lector 35, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.
- h) Postul de Lector 36, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.

Membrii Consiliului Departamentului de Informatică au respins cu unanimitate de voturi următoarea propunere:

- c) Postul de Asistent 69, prevăzut în statul de funcții al Departamentului de Informatică, anul 2024-2025 - vacant, scos la concurs.

Director Departament Informatică,
pentru Lector Dr. Adriana Loredana Tănăsie
Lector Dr. Cira Cristian



Extras din proces verbal

DECANAT

Încheiat în data de 12.03.2025, ora 16:20, ședința extraordinară a Consiliului Facultății de Matematică și Informatică, prin procedura votului electronic, cu următoarea ordine de zi:

1. *Aviz pentru finalizarea studiilor pentru studenți din promoții anterioare.*
2. *Aviz pentru solicitările de echivalări a studenților: A. Rosoga, T. Minda, M. Nastasi, P. Sinoi, A. Tamasi, M. Mihailescu, M. Corojoar, V. Tudor.*
3. *Aviz pentru modificarea standardelor minimale de Matematica*
4. *Aviz pentru **modificarea** modalității de ocupare a postului didactic vacant de **Lector universitar 33**, din statul de funcții al Departamentului de Informatică, pentru anul universitar 2024-2025 din vacant promovare în **vacant concurs**.*
5. *Aviz pentru scoaterea la concurs pentru Semestrul II a posturilor de Asistent 66, Asistent 68 pentru perioada determinată din statul de funcții a Departamentului de Informatică (dosarele pentru posturi)*
6. *Aviz pentru scoaterea la concurs pentru Semestrul II a posturilor de Lector 32, Lector 33, Lector 34, Lector 35, Lector 36 din statul de funcții a Departamentului de Informatică (dosarele pentru posturi)*

Rezoluție vot electronic:

= omis cele de omis =

Punctul 3 (modificarea standardelor minimale de Matematica) a fost avizat cu un număr de 12 voturi de acord.

= omis cele de omis =

Decan,
Conf. univ. dr. Cosmin Bonchiș



Întocmit secretar șef,
Ancuța-Sanda Eduțanu



Extras din proces verbal

DECANAT

Încheiat în data de 12.03.2025, ora 16:20, ședința extraordinară a Consiliului Facultății de Matematică și Informatică, prin procedura votului electronic, cu următoarea ordine de zi:

1. *Aviz pentru finalizarea studiilor pentru studenți din promoții anterioare.*
2. *Aviz pentru solicitările de echivalări a studenților: A. Rosoga, T. Minda, M. Nastasi, P. Sinoi, A. Tamasi, M. Mihailescu, M. Coroior, V. Tudor.*
3. *Aviz pentru modificarea standardelor minimale de Matematica*
4. *Aviz pentru **modificarea** modalității de ocupare a postului didactic vacant de **Lector universitar 33**, din statul de funcții al Departamentului de Informatică, pentru anul universitar 2024-2025 din vacant promovare în **vacant concurs**.*
5. *Aviz pentru scoaterea la concurs pentru Semestrul II a posturilor de Asistent 66, Asistent 68 pentru perioada determinată din statul de funcții a Departamentului de Informatică (dosarele pentru posturi)*
6. *Aviz pentru scoaterea la concurs pentru Semestrul II a posturilor de Lector 32, Lector 33, Lector 34, Lector 35, Lector 36 din statul de funcții a Departamentului de Informatică (dosarele pentru posturi)*

Rezoluție vot electronic:

= omis cele de omis =

Punctul 4 (modificarea modalității de ocupare a postului didactic vacant de Lector universitar 33, din statul de funcții al Departamentului de Informatică, pentru anul universitar 2024-2025 din vacant promovare în vacant concurs) a fost avizat cu un număr de 12 voturi de acord.

= omis cele de omis =

Decan,
Conf. univ. dr. Cosmin Bonchiș

Întocmit secretar șef,
Ancuța-Sanda Eduțanu



Extras din proces verbal

DECANAT

Încheiat în data de 12.03.2025, ora 16:20, ședința extraordinară a Consiliului Facultății de Matematică și Informatică, prin procedura votului electronic, cu următoarea ordine de zi:

1. *Aviz pentru finalizarea studiilor pentru studenti din promotii anterioare.*
2. *Aviz pentru solicitarile de echivalari a studentilor: A. Rosoga, T. Minda, M. Nastasi, P. Sinoi, A. Tamasi, M. Mihailescu, M. Coroior, V. Tudor.*
3. *Aviz pentru modificarea standardelor minimale de Matematica*
4. *Aviz pentru **modificarea** modalității de ocupare a postului didactic vacant de **Lector universitar 33**, din statul de funcții al Departamentului de Informatică, pentru anul universitar 2024-2025 din vacant promovare în **vacant concurs**.*
5. *Aviz pentru scoaterea la concurs pentru Semestrul II a posturilor de Asistent 66, Asistent 68 pentru perioada determinata din statul de funcții a Departamentului de Informatică (dosarele pentru posturi)*
6. *Aviz pentru scoaterea la concurs pentru Semestrul II a posturilor de Lector 32, Lector 33, Lector 34, Lector 35, Lector 36 din statul de funcții a Departamentului de Informatică (dosarele pentru posturi)*

Rezoluție vot electronic:

= omis cele de omis =

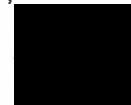
Punctul 5 (scoaterea la concurs pentru Semestrul II a posturilor de Asistent 66, Asistent 68 pentru perioada determinata din statul de funcții a Departamentului de Informatică (dosarele pentru posturi)) a fost avizat cu un numar de 12 voturi de acord.

= omis cele de omis =

Decan,
Conf. univ. dr. Cosmin Bonchis



Întocmit secretar șef,
Ancuța-Sanda Eduțanu



Extras din proces verbal

DECANAT

Încheiat în data de 12.03.2025, ora 16:20, ședința extraordinară a Consiliului Facultății de Matematică și Informatică, prin procedura votului electronic, cu următoarea ordine de zi:

1. *Aviz pentru finalizarea studiilor pentru studenți din promoții anterioare.*
2. *Aviz pentru solicitările de echivalări a studenților: A. Rosoga, T. Minda, M. Nastasi, P. Sinoi, A. Tamasi, M. Mihailescu, M. Corojoș, V. Tudor.*
3. *Aviz pentru modificarea standardelor minimale de Matematica*
4. *Aviz pentru **modificarea** modalității de ocupare a postului didactic vacant de **Lector universitar 33**, din statul de funcții al Departamentului de Informatică, pentru anul universitar 2024-2025 din vacant promovare în **vacant concurs**.*
5. *Aviz pentru scoaterea la concurs pentru Semestrul II a posturilor de Asistent 66, Asistent 68 pentru perioada determinată din statul de funcții a Departamentului de Informatică (dosarele pentru posturi)*
6. *Aviz pentru scoaterea la concurs pentru Semestrul II a posturilor de Lector 32, Lector 33, Lector 34, Lector 35, Lector 36 din statul de funcții a Departamentului de Informatică (dosarele pentru posturi)*

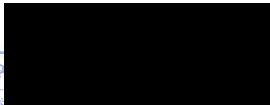
Rezoluție vot electronic:

= omis cele de omis =

Punctul 6 (scoaterea la concurs pentru Semestrul II a posturilor de Lector 32, Lector 33, Lector 34, Lector 35, Lector 36 din statul de funcții a Departamentului de Informatică (dosarele pentru posturi)) a fost avizat cu un număr de 12 voturi de acord.

= omis cele de omis =

Decan,
Conf. univ. dr. Cosmin Bonchiș



Întocmit secretar șef,
Ancuța-Sanda Eduțanu

