Securitatea Informației 2017

Subiectele de mai jos vizeaza principii generale ce trebuiesc cunoscute, necerandu-se reproducerea exacta a structurii mesajelor sau regulile protocoalelor implicate in cadrul acestora.

Daca un subiect de examen, diferit de cele de mai jos, va viza anumite aspecte strans legate de structura unui protocol din curs, atunci acest protocol va fi prezentat explicit ca ipoteza de lucru in enuntul subiectului.

De exemplu, daca se cere o analiza de securitate asupra protocolului Kerberos, atunci acest protocol va fi prezentat ca ipoteza de lucru in enuntul subiectului.

Sisteme de protecție

1. Ce este un sistem de protectie peste o multime de drepturi (definiti toate conceptele ce intervin in explicarea conceptului de sistem de protectie)
2. In ce consta problema sigurantei sistemelor de protectie?
3. Ce cunoasteti despre dificultatea rezolvarii algoritmice a problemei sigurantei sistemelor de protectie?
4. Ce este o lista de control al accessului? Discutati cazul UNIX si WINDOWS NT.
5. Ce este o lista de capacitati?
6. Ce intelegeti prin acces discretionar si acces mandatar?
7. **Subiectul 2016a, ex 1**

(Politici de securitate – timp estimat: 40')

(a) Descrieţi modelul Bell-LaPadula (explicaţi clar fiecare notaţie utilizată). **10p**

(b) Descrieţi modelul Biba (explicaţi clar fiecare notaţie utilizată). **10p**

(c) In Figura 1 aveţi două latici de clase de securitate. Utilizaţi una dintre ele pentru a ilustra modelul Bell-LaPadula, iar cealaltă pentru modelul Biba.

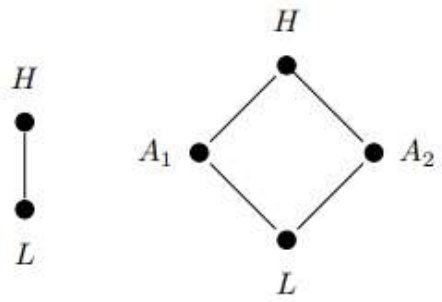

Figure 1: Latici de securitate

5p

(d) Combinaţi modelele de la punctul anterior într-un singur model şi explicaţi-l. **10p**

8. Subiectul 2016b, ex 1

(Controlul accesului – timp estimat: 40')

(a) Care sunt operaţiile primitive în cadrul modelului bazat pe matrici de control al accesului? **5p**

(b) Ce se înţelege prin comandă în cadrul modelului bazat pe matrici de control al accesului? **5p**

(c) Ce se înţelege prin sistem de protecţie în cadrul modelului bazat pe matrici de control al accesului? **5p**

(d) Fie structurile

command $CREATE(process, file)$
  if *file does not exist*
  then
    create object *file*
    enter own into $(process, file)$
end

command $CONFER\_READ(owner, friend, file)$
  if *own in* $(owner, file)$ *and*
    r *not in* $(friend, file)$
  then
    create object *file*
    enter x *into* $(friend, file)$
end

Este $\mathcal{C} = \{CREATE, CONFER\_READ\}$ sistem de protecţie peste mulţimea de drepturi $R = \{own, r, w\}$? Justificaţi răspunsul. **5p**

(e) Fie comanda $JUST\_CREATE$ peste mulţimea de drepturi $R = \{f, m, r, w\}$ dată prin

command $JUST\_CREATE(X_{s_1}, X_{s_2}, X_o)$
  if f *in* (X_{s_1}, X_{s_2}) *and*
    m *in* (X_{s_2}, X_{s_1})
  then
    create object X_o
end

şi A matricea de control al accesului de mai jos

	Ion	Gelu	Dan	*file*
Ion	r	r, w, f	r, a	$\emptyset$
Gelu	w, m	r, w	r, a	r
Dan	r	$\emptyset$	$\emptyset$	w

Se poate aplica $JUST\_CREATE(Ion, Gelu, personal)$ asupra matricii A? Dacă da, care este rezultatul? Justificaţi răspunsul. **5p**

(f) Este posibil a aplica comanda $JUST\_CREATE$ de la punctul anterior unei matrici de control al accesului ce are doar un singur subiect? Justificaţi răspunsul. **5p**

(g) Fie $\mathcal{C} = \{JUST\_CREATE\}$ un sistem de protecţie peste $R = \{f, m, r, w\}$, şi fie $Q = (S, O, A)$ starea dată prin $S = \{$Ion,Gelu,Dan$\}$, $O = \{$Ion,Gelu,Dan, $file\}$ şi matricea A de la punctul (e). Este Q sigură pentru dreptul f? Justificaţi răspunsul. **5p**

9. Subiectul 2016c, ex 1

(Controlul accesului – timp estimat: 40')

(a) Care sunt operaţiile primitive în cadrul modelului take-grant de control al accesului ? (Specificaţi clar în cadrul fiecărei operaţii tipul părţilor implicate în aceasta (subiect/obiect)). **10p**

(b) Ce se înţelege prin comandă în cadrul modelului bazat pe matrici de control al accesului? **10p**

(c) Arătaţi că orice sistem de protecţie take-grant poate fi simulat printr-un sistem de protecţie bazat pe matrici de access al controlului, prin păstrarea proprietăţii de siguranţă (dacă un drept este sigur într-un sistem atunci el este sigur şi în celălalt). **25p**

10. Subiectul 2015b, ex 3

(Controlul accesului – timp estimat 30') Arătaţi că pentru orice graf orientat finit $G = (V, E)$ se poate construi, în timp polinomial în raport cu dimensiunea grafului, un sistem de protecţie mono-operaţional peste o mulţime R de drepturi, o stare Q a acestuia şi se poate specifica un drept $r \in R$ astfel încât G admite o clică de dimensiune k ($k \leq |V|$) dacă şi numai dacă Q nu este sigură pentru r. **3p**

11. **Subiectul 2013g, ex 3 (RESTANTA SPECIALA)**

Considerăm, în cadrul modelului take-grant, două insule (distincte) I_1 şi I_2 conectate printr-un element extern z.

- Discutaţi posibilitatea şi modul de transfer a drepturilor de la o insulă la cealaltă. **7p**
- Studiaţi complexitatea algoritmului prin care o insulă poate obţine toate drepturile celeilalte insule. **8p**

IPsec

1. Ce este o asociere de securitate in IPsec si care sunt mecanisemele de securitate fundamentale din IPsec?
2. Descrieti, succint dar clar, protocolul AH in cele doua moduri de utilizare pentru datagrame IPv4.
3. Descrieti, succint dar clar, protocolul ESP ın cele doua moduri de utilizare pentru datagrame IPv4.
4. Descrieti cateva combinatii de asocieri de securitate in IPsec (end-to-end, VPN, end-to-end cu VPN).
5. **Subiectul 2016a, ex 3**

(IPsec – timp estimat: 40')
Descriem mai jos un posibil atac asupra modului de operare CBC în IPsec. In acest mod, o secvenţă de blocuri $x = x_1 \cdots x_n$ se criptează cu o cheie K prin $y = y_1 \cdots y_n$, unde $y_1 = e_K(x_1 \oplus x_0)$, x_0 este un vector de iniţializare dat, iar $y_{i+1} = e_k(x_{i+1} \oplus y_i)$ pentru orice $i \geq 1$.

Constatăm că dacă alterăm un bit în y_2, atunci acelaşi bit va fi alterat în x_3 (la decriptare) deoarece $x_3 = y_2 \oplus d_K(y_3)$. Presupunând că primii 32 biţi din x_3 vor trebui să conţină adresa IP destinaţie, atacantul poate modifica primii 32 biţi ai lui y_2 astfel încât, prin decriptare, primii 32 de biţi ai lui x_3 să conţină adresa atacantului.

(a) Detaliaţi atacul de mai sus arătând clar cum se poate modifica y_2 (presupunem că atacantul are acces la mesajul criptat). **10p**

(b) Presupunem că în IPsec modul de criptare CBC se înlocuieşte cu modul de criptare OFB unde $y_i = e_K^i(x_0) \oplus x_i$, pentru orice $i \geq 1$.
Mai funcţionează atacul de la (a) în acest caz ? **10p**

(c) Presupunem că în IPsec modul de criptare CBC se înlocuieşte cu modul de criptare CFB unde $y_0 = x_0$ şi $y_i = e_K(y_{i-1}) \oplus x_i$, pentru orice $i \geq 1$.
Mai funcţionează atacul de la (a) în acest caz ? **10p**

6. **Subiectul 2016b, ex 2**

(IPsec – timp estimat: 40')

(a) Descrieţi, succint dar clar, elementele ce stau la baza arhitecturii *IPsec* (asociere de securitate, AH, ESP, moduri de utilizare pentru datagrame IPv4). **15p**

(b) Modul de criptare CBC al unei secvenţe $P_1 \cdots P_n$ cu vectorul de iniţializare $IV = C_0$ este dat prin $C_i = e_K(P_i \oplus C_{i-1})$, pentru orice $1 \leq i \leq n$. Ce implicaţii, la destinaţie, are apariţia unei erori în transmisia unui bloc C_i ? **10p**

(c) Modul de criptare PCBC al unei secvenţe $P_1 \cdots P_n$ cu vectorul de iniţializare $IV = C_0$ este dat prin $C_1 = e_K(P_1 \oplus C_0)$ şi $C_i = e_K(P_i \oplus P_{i-1} \oplus C_{i-1})$, pentru orice $2 \leq i \leq n$. Ce implicaţii, la destinaţie, are apariţia unei erori în transmisia unui bloc C_i ? **10p**

7. Subiectul 2016c, ex 2

(Distribuţia cheii, IPsec – timp estimat: 40')
Considerăm următoarea schemă de distribuţie a cheii pentru n utilizatori. Administratorul (TA) alege un număr prim $p > n$, trei coeficienţi $a, b, c \in \mathbf{Z}_p$ (distincţi doi câte doi) şi formează polinomul

$$f(x, y) = a + b(x + y) + cxy \ mod \ p.$$

TA distribuie fiecărui utilizator U polinomul

$$g_U(x) = f(x, r_U) \ mod \ p = a_U + b_U x \ mod \ p,$$

unde $r_U \in \mathbf{Z}_p$ este un parametru public ales random de U. Polinomul g_U este secret al lui U.
Doi utilizatori U şi V vor comunica prin intermediul cheii

$$K_{UV} = g_U(r_V) = f(r_U, r_V) = f(r_V, r_U) = g_V(r_U) = K_{VU}$$

ce o pot calcula independent.

(a) Arătaţi că schema este rezistentă la atac de coaliţie 1 (niciun utilizator nu poate determina, cu probabilitate ne-neglijabilă polinomul secret al altui utilizator). **(15p)**

(b) Este schema rezistentă la atac de coaliţie 2 ? (Justificaţi răspunsul). Dacă schema nu este rezistentă la atac de coaliţie 2, modificaţi-o astfel încât aceasta să fie rezistentă la atac de coaliţie 2. **(20p)**

(c) Descrieţi o modalitate prin care componenta IKE a protocolului IPsec poate fi modificată prin includerea schemei de la punctul precedent, şi studiaţi securitatea ei. Discutaţi apoi avantajele şi dezavantajele acestei noi metode în comparaţie cu metoda IKE standard. **(20p)**

8. Subiectul 2016d, ex 2

(IPsec – timp estimat: 40')
Modul CFB de criptare a unei secvenţe binare x cu un criptosistem pentru care lungimea cheii de criptare, a blocului de intrare şi a celui de ieşire este m, funcţionează astfel:

- se împarte x în blocuri de lungime r, $x = x_1 \cdots x_n$, unde $1 \leq r \leq m$;
- se consideră un vector de iniţializare de lungime m;
- se aplică următorul algoritm ce produce criptotextul y asociat lui x cu cheia K:

$I_0 := IV$;
$y_0 := \lambda$; (λ este şirul vid)
$y := \lambda$;
for $j := 1$ **to** n **do**
    $I_j :=$ ultimii m bits ai lui $I_{j-1}y_{j-1}$
    $z_j :=$ primii r bits ai lui $e_K(I_j)$;
    $y_j := x_j \oplus z_j$;
    $y := yy_j$;
end_for

(a) Cum se realizează decriptarea în modul CFB? **15p**

(b) Descriem mai jos un posibil atac asupra modului de operare CBC în IPsec. In acest mod, o secvenţă de blocuri $x = x_1 \cdots x_n$ se criptează cu o cheie K prin $y = y_1 \cdots y_n$, unde $y_1 = e_K(x_1 \oplus x_0)$, x_0 este un vector de iniţializare dat, iar $y_{i+1} = e_k(x_{i+1} \oplus y_i)$ pentru orice $i \geq 1$.
Constatăm că dacă alterăm un bit în y_2, atunci acelaşi bit va fi alterat în x_3 (la decriptare) deoarece $x_3 = y_2 \oplus d_K(y_3)$. Presupunând că primii 32 biţi din x_3 vor trebui să conţină adresa IP destinaţie, atacantul poate modifica primii 32 biţi ai lui y_2 astfel încât, prin decriptare, primii 32 de biţi ai lui x_3 să conţină adresa atacantului. Cum ? **15p**

(c) Dacă în IPsec se utilizează modul de criptare CFB în locul modului CBC, se mai poate monta atacul de la punctul precedent ? **25p**

9. **Subiectul 2015b, ex 2**

(IPsec – timp estimat 30') Presupunem că ESP în modul transport încapsulează segmente TCP, iar aceste segmente sunt criptate în modul CBC. Dacă un intrus are acces (citire şi modificare) la vectorul de iniţializare IV al modului de criptare, poate acesta monta un atac cu succes? Discutaţi toate variantele posibile ce credeţi că pot conduce la atac, şi argumentaţi-le cât mai riguros. **3p**

Notă: Structura unui segment TCP este cea de mai jos:

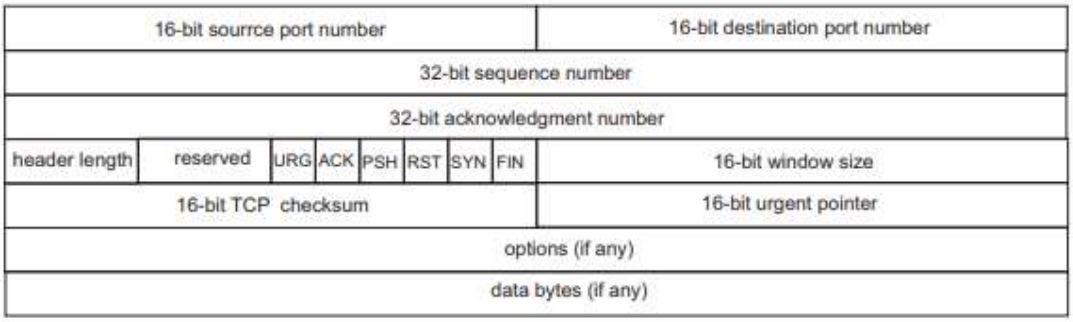

Figure 2: Format segment TCP

10. **Subiectul 2015c, ex1**

(*IPsec*)

(a) Descrieţi, succint dar clar, elementele ce stau la baza arhitecturii *IPsec* (asociere de securitate, AH, ESP, moduri de utilizare pentru datagrame IPv4). **3p**

(b) Modul de criptare CBC al unei secvenţe $P_1 \cdots P_n$ cu vectorul de iniţializare $IV = C_0$ este dat prin $C_i = e_K(P_i \oplus C_{i-1})$, pentru orice $1 \leq i \leq n$. Ce implicaţii, la destinaţie, are apariţia unei erori în transmisia unui bloc C_i? **1p**

(c) Modul de criptare PCBC al unei secvenţe $P_1 \cdots P_n$ cu vectorul de iniţializare $IV = C_0$ este dat prin $C_1 = e_K(P_1 \oplus C_0)$ şi $C_i = e_K(P_i \oplus P_{i-1} \oplus C_{i-1})$, pentru orice $2 \leq i \leq n$. Ce implicaţii, la destinaţie, are apariţia unei erori în transmisia unui bloc C_i? **1p**

SSL/TLS

1. Care este scopul de baza a protocolului SSL/TLS?
2. Descrieti, succint dar clar, metodele de schimb de cheie RSA si DH in SSL.
3. Care sunt pasii de baza ai protocolului “SSL record”?

4. **Subiectul 2015c, ex 2**

Presupunem că mesajele transmise prin SSL sunt prelucrate astfel:

- mesajul este împarţit în blocuri, $B_1, \ldots, B_m$ (fiecare cu cel mult 2^{14} octeţi);
- pentru fiecare bloc B_i se realizează:
  - se aplică un MAC blocului B_i rezultând X_i;
  - se criptează X_i cu un criptosistem simetric în modul CBC rezultând Y_i;
  - se adaugă un header SSL rezultând Z_i;
  - se transmite Z_i printr-un segment TCP.

Criptarea primului bloc X_1 se face astfel:

- se împarte X_1 în blocuri de 64 sau 128 bits (în funcţie de criptosistem), $X_1 = x_1^1 \cdots x_1^{l_1}$;
- se generează $Y_1 = y_1^1 \cdots y_1^{l_1}$, unde $y_1^1 = e_k(x_1 \oplus y_0)$, y_0 este un vector iniţial, iar $y_1^j = e_K(x_1^j \oplus y_1^{j-1})$, pentru orice $j > 1$.

Criptarea celorlalte blocuri $X_i = x_i^1 \cdots x_i^{l_i}$ $(i > 1)$ se face ca şi pentru X_1 dar cu deosebirea că y_0 este ales ca fiind $y_{i-1}^{l_{i-1}}$ (ultimul criptotext din blocul anterior).

(a) Arătaţi că un intrus care are acces la blocurile Y_1 şi X_2 dar nu la X_1, poate decide efectiv dacă un anumit sub-bloc x_1^j coincide sau nu cu un mesaj x^* (de aceeaşi lungime cu x_1^j) ales de intrus (remarcă: funcţia de criptare este injectivă). **2p**

(b) Dacă un sub-bloc x_1^j conţine o parolă mică, poate fi utilizat rezultatul anterior pentru montarea unui atac prin ghicirea parolei? (puteţi presupune că intrusul poate monta un atac de plaintext ales). **1.5p**

(c) Cum poate fi îmbunătăţit protocolul pentru a nu mai avea loc proprietatea de la (a)? **1.5p**

DNS si DNSsec

1. Descrieti, succint dar clar, modul de functionare a protocolului DNS.
2. Descrieti, succint dar clar, modul de functionare a protocolului DNSsec.
3. Prezentati si discutati 2 argumente pentru care credeti ca DNSsec asigura securitate.
4. **Subiectul 2016a, ex 2**

(DNSsec – timp estimat: 40')
In Figura 2 aveţi un arbore DNS (mult simplificat) în care sunt figurate zonele de autoritate (prin elipse întrerupte – nodul rădăcină este zona de autoritate pentru el). Se presupune că nodul `example` conţine inregistrări de tip SOA, MX şi NS, nodurile `cc` şi `cdc` conţin fiecare înregistrări de tip NS şi MX, iar nodurile copil a nodurilor `cc` şi `cdc` conţin înregistrări de tip A. Cerinţe:

(a) Care sunt serviciile fundamentale asigurate de DNSsec? **3p**

(b) Care sunt înregistrările introduse de DNSsec? **8p**

(c) Arătaţi cum se adaugă înregistrările specifice DNSsec arborelui din Figura 2. **8p**

(d) Explicaţi cum se obţin proprietăţile de securitate DNSsec pentru rezoluţia `c2.cc.example` **8p**

(e) Explicaţi cum se obţin proprietăţile de securitate DNSsec pentru rezoluţia `c2.ccc.example` **8p**

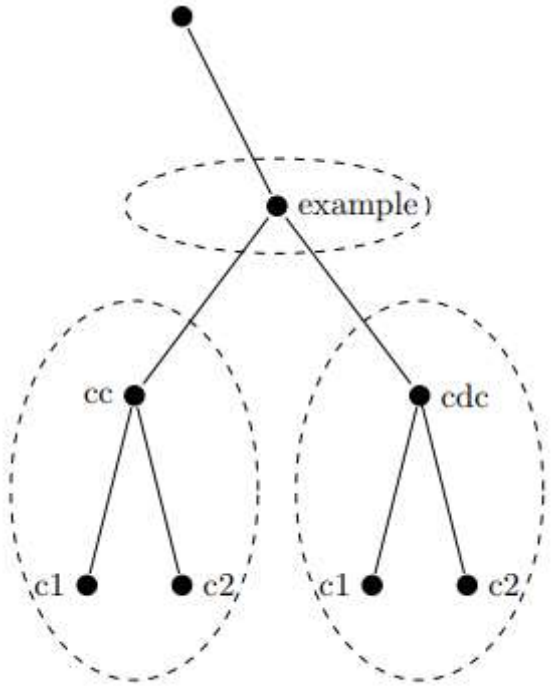

Figure 2: Arbore DNS

5. **Subiectul 2015a, ex 3**

(DNSsec – timp estimat: 30')
In Figura 1 aveti un arbore DNS (mult simplificat) în care sunt figurate zonele de autoritate (prin elipse întrerupte – nodul rădăcină este zona de autoritate pentru el). Se presupune ca nodul `example` conţine

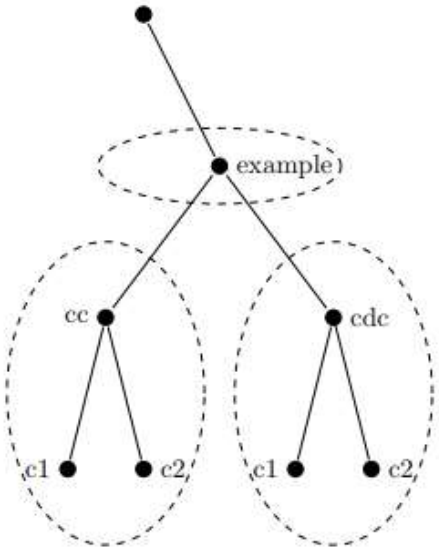

Figure 1: Arbore DNS

inregistrări de tip SOA, MX şi NS, nodurile `cc` şi `cdc` conţin fiecare înregistrări de tip NS şi MX, iar nodurile copil a nodurilor `cc` şi `cdc` conţin înregistrări de tip A. Cerinţe:

(a) Care sunt serviciile fundamentale asigurate de DNSsec? **0.25p**
(b) Arătaţi cum se adaugă înregistrările specifice DNSsec arborelui din Figura 1. **0.75p**
(c) Explicaţi cum se obţin proprietăţile de securitate DNSsec pentru rezoluţia `c2.cc.example` **1p**
(d) Explicaţi cum se obţin proprietăţile de securitate DNSsec pentru rezoluţia `c2.ccc.example` **1p**

Pretty Good Privacy (PGP)

1. Ce servicii ofera PGP?
2. Cum se realizeaza autentificarea in PGP?
3. Cum se asigura confidentialitatea in PGP?
4. Cum se realizeaza autentificarea si confidentialitatea, impreuna, in PGP?

5. Cum se realizeaza compresia informatiei in PGP?
6. Explicati modul de formare si utilizare a inelelor de chei in PGP.
7. **Subiectul 2014a, ex2**

   (PGP – timp estimat: 30')

   (a) Ce servicii oferă PGP? **0.5p**
   (b) Cum se realizează autentificarea în PGP? **0.5p**
   (c) Cum se asigură confidenţialitatea în PGP? **1p**
   (d) Cum se realizează autentificarea şi confidenţialitatea, împreună, în PGP? **1p**
   (e) Explicaţi modul de formare şi utilizare a inelelor de chei in PGP. **1p**

8. **Subiectul 2016d, ex 1**

   (Controlul accesului – timp estimat: 40')

   (a) Cum se realizează autentificarea şi confidenţialitatea în cadrul PGP ? Descrieţi şi modul de administrare a cheilor necesare. **15p**
   (b) Presupunem că în modul "autentificare şi confidenţialitate" în PGP inversăm operaţiile (de autentificare şi confidenţialitate). Crează aceasta vreo problemă relativ la autentificare şi confidenţialitate? Explicaţi aceasta prin comparaţie cu protocolul original. **15p**
   (c) Presupunem că operaţia de autentificare în PGP este realizată doar prin hash. Se păstrează proprietatea de autentificare? Explicaţi aceasta prin comparaţie cu protocolul original. **15p**

S/MIME

1. Cum se realizeaza autentificarea in S/MIME? (atentie: exista doua tipuri de autentificare in S/MIME).
2. Cum se asigura confidentialitatea in S/MIME?
3. Cum se realizeaza autentificarea si confidentialitatea, impreuna, in S/MIME?

RFC 822 si MIME

1. Care sunt principalele dezavantaje ale formatului de e-mail RFC 822?
2. Care este structura de baza a unui format MIME?
3. Care sunt cele 4 metode de codificare a informatiei in MIME?
4. In ce consta metoda de codificare "quoted-printable"?
5. In ce consta metoda de codificare Radix64?

Elemente de criptografie

1. Ce este un criptosistem simetric?
2. Ce este un criptosistem asimetric (cu chei publice)?
3. Care este diferenta majora intre un criptosistem simetric si unul cu chei publice?
4. Ce este o functie hash?
5. Ce este o semnatura digitala? Cum se construieste semnatura digitala RSA?
6. In ce consta metoda de demonstratie challenge-and-response?
7. Ce se intelege prin zero-knowledge-proof?

Altele

1. Subiectul 2016b, ex 3

(Timp estimat: 40')
Problema *Cinei criptografilor* se formulează astfel. Trei criptografi, C_1, C_2 şi C_3 au luat cina şi, la sfârşit, au fost anunţaţi că cineva a plătit. Cum masa putea fi plătită de un criptograf (şi doar de unul) sau de o persoană externă, criptografii hotărăsc să afle dacă cina a fost plătită de un extern sau de unul dintre ei dar, în cel de-al doilea caz, să nu se divulge identitatea acestuia. Pentru aceasta ei procedează conform următorului protocol, notat $DC(3)$:

- fiecare criptograf C_i alege random un bit şi îl comunică în mod secret criptografului din stânga sa (criptografii sunt asezaţi la o masă circulară în ordinea C_1, C_2, C_3, de la stânga la dreapta);
- fiecare criptograf C_i alege încă un bit astfel: bitul 0 dacă nu a plătit masa, şi 1, altfel;
- fiecare criptograf C_i publică suma modulo 2 ($\oplus$) a celor 3 bits cunoscuţi, notată z_i.

In urma desfăşurării protocolului şi analizei sumei $z_1 \oplus z_2 \oplus z_3$, criptografii deduc dacă masa a fost plătită de unul dintre ei sau de un extern. In plus, din punctul de vedere al unui criptograf ce nu a plătit masa, oricare din ceilalţi doi criptografi ar fi putut să o plătească, cu egală probabilitate (în ipoteza în care unul dintre ei a plătit-o).

(a) Justificaţi corectitudinea concluziei criptografilor (presupunând că criptografii sunt oneşti în cadrul protocolului $DC(3)$). **10p**

(b) Generalizaţi problema de mai sus la cazul a $n \geq 3$ criptografi (protocolul va fi notat $DC(n)$). **5p**

(c) In cadrul protocolului $DC(n)$, $n \geq 3$, presupunem că criptografii C_{i-1} şi C_{i+1} bănuiesc că C_i a plătit masa. Dacă C_{i-1} şi C_{i+1} îşi pun în comun o parte din informaţiile lor private, pot ei stabili dacă C_i a plătit sau nu? Justificaţi răspunsul. (în cadrul notaţiei de mai sus, dacă $i = 1$ atunci $i - 1$ va fi considerat n, iar dacă $i = n$ atunci $i + 1$ va fi considerat 1). **10p**

(d) Protocolul $DC(n)$ are dezavantajul că dacă un criptograf a plătit masa dar cel puţin un alt criptograf C_i nu este onest în publicarea valorii reale (corecte) z_i, atunci concluzia desprinsă de criptografi poate fi eronată. Justificaţi aceasta. **5p**

2. Subiectul 2015a, ex 2

(Protocolul Woo-Lam – timp estimat: 30')
Protocolul de mai jos are scopul de a mijloci autentificarea unui client A către un alt client B prin intermediul unui server S (în protocol, $\{x\}_K$ înseamnă x criptat cu K, iar K_{XY} reprezintă cheia partajată de X şi Y):

1. $A \rightarrow B$: A
2. $B \rightarrow A$: N_b
3. $A \rightarrow B$: $\{A, B, N_b\}_{K_{AS}}$
4. $B \rightarrow S$: $\{A, B, \{A, B, N_b\}_{K_{AS}}\}_{K_{BS}}$
5. $S \rightarrow B$: $\{A, B, N_b\}_{K_{BS}}$

- Explicaţi modul în care funcţionează protocolul (furnizaţi cât mai multe detalii convingătoare asupra realizării obiectivului acestuia). **0.5p**
- Se ştie că acest protocol este vulnerabil la atac prin interpunerea unui intrus între participanţii la protocol. Prezentaţi un astfel de atac. **2.5p**

3. Subiectul 2014a, ex 3

(Managementul cheii – timp estimat: 30')
Considerăm următoarea metodă de partajare a unei parole $K \in \mathbf{Z}_m$ la n participanţi:

(a) se aleg random $n - 1$ numere $a_1, \ldots, a_{n-1} \in \mathbf{Z}_m$ şi se distribuie (pe un canal secret) la $n - 1$ participanti;

(b) celui de al n-lea participant i se distribuie $(K - \sum_{i=1}^{n-1} a_i) \ mod \ m$.

Arătaţi urmatoarele:

(a) Dacă $m > n$ atunci schema este rezistentă la atac de coaliţie $n - 1$ (dacă $n - 1$ participanţi pun în comun secretele lor parţiale, atunci ei nu obţin nici o informaţie suplimentară asupra cheii partajate); **1.25p**

(b) Cerinţa ca m să fie prim ar îmbunătăţi schema? Justificaţi răspunsul. **0.25p**

(c) Rezultatul de la (1) se mai păstrează dacă $m \leq n$? Justificaţi răspunsul. **0.5p**

4. Subiectul 2014c, ex 3

(Schimbul cheii – timp estimat: 20')

(a) Descrieţi metoda Diffie-Hellman de schimb de cheie (explicaţi clar elementele utilizate). **0.50p**

(b) Este metoda Diffie-Helman de schimb de cheie sigură? Justificaţi răspunsul. **0.75p**

(c) Ce variante ale metodei Diffie-Helman de schimb de cheie cunoaşteţi, în ce protocol le-aţi întâlnit, şi ce puteţi spune despre securitatea lor. **0.75p**

5. Subiectul 2013g, ex 1 (RESTANTA SPECIALA)

In ce constă paradoxul zilei de naştere şi care este importanţa lui în construcţia de funcţii hash rezistente la coliziuni? **10p**

6. Subiectul 2013g, ex 2 (RESTANTA SPECIALA)

Considerăm următoarea schemă de distribuţie a cheii pentru n utilizatori. Administratorul (TA) alege un număr prim $p > n$, generează random trei coeficienţi $a, b, c \in \mathbf{Z}_p$ (distincţi doi câte doi) şi formează polinomul

$$f(x, y) = a + b(x + y) + cxy \ mod \ p.$$

TA distribuie fiecărui utilizator U polinomul

$$g_U(x) = f(x, r_U) \ mod \ p = a_U + b_U x \ mod \ p,$$

unde $r_U \in \mathbf{Z}_p$ este un parametru public ales random de U. Polinomul g_U este secret al lui U.

Doi utilizatori U şi V vor comunica prin intermediul cheii

$$K_{UV} = g_U(r_V) = f(r_U, r_V) = f(r_V, r_U) = g_V(r_U) = K_{VU}.$$

Arătaţi următoarele:

(a) Schema este rezistentă la atac de coaliţie 1 (pentru un utilizator W, cheia utilizată de orice alţi doi utilizatori poate fi oricare din cheile posibile, cu aceeaşi probabilitate). **7p**

(b) Schema nu este rezistentă la atac de coaliţie 2 (doi utilizatori pot deduce în timp polinomial cheia utilizată de orice alţi doi utilizatori). **8p**