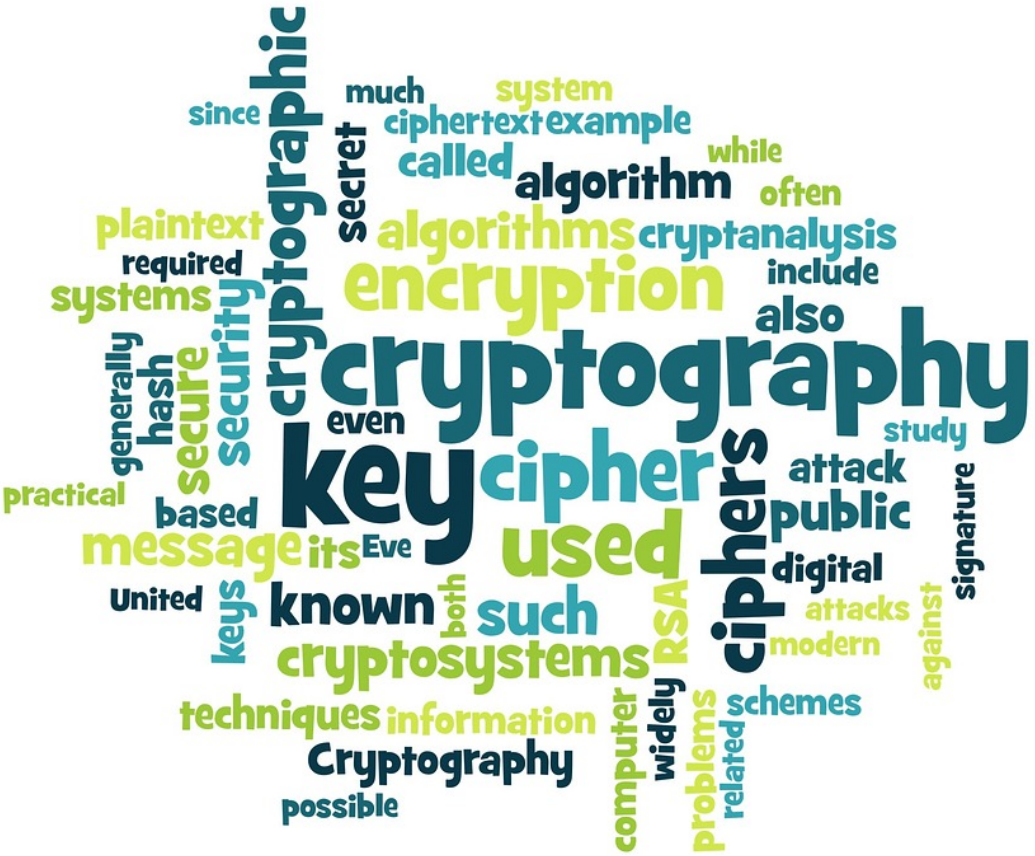

Securitatea Rețelelor de Calculatoare
PROIECTE TIP I

Conf.Univ.Dr. Nicolae Constantinescu

Craiova, 17 martie 2016.

Mod de elaborare a proiectelor:

Un student poate alege orice proiect. Acesta va fi elaborat implementând codul aferent într-un limbaj de programare. Proiectul va trebuii să conţina comentarii care să descrie algoritmii folosiţi, funcţionalitatea, modul de rezolvare şi să lucreze independent de librăriile instalate pe un sistem de calcul.

Proiectul va fi prezentat public şi se vor puncta:

a. Originalitatea implementării
b. Eficienţa proiectului în piaţa reală a software-urilor de profil

Proiect 1

Tema 1

Fie sistemul (P, C, K, e, d) unde:

- P este textul iniţial care tebuie criptat, fiind format din unul sau mai multe cuvinte alcătuite din litere ce aparţin mulţimii $\{a, b, c \dots z\}$.
- C este textul ce se va obţine în urma criptării. Literele aparţin aceleiaşi mulţimi ca şi literele lui P.
- K este un număr asupra caruia vor cădea de comun acord cei care vor să comunice. Pe baza lui K se va face criptarea, K fiind, într-un cuvânt, cheia secretă.
- e este funcţia de criptare definită astfel $P \times K \to C$ $e(P, K) = (P + K)(mod\ m) = C$ unde m este lungimea alfabetului folosit.
- d este funcţia de decriptare definită astfel $C \times K \to P$ $d(C, K) = (C - K)(mod\ m) = P$ unde m este lungimea alfabetului folosit.

Sistemul de mai sus este cunoscut ca Sistemul lui Caesar.

Cerinţe:

1. Pornind de la acest sistem implementaţi un algoritm pentru el. Algoritmul trebuie să conţină funcţie de criptare, funcţie de decriptare, generator de chei pe baza unei parole.
2. Să se facă o criptanaliză pentru determinarea vulnerabilităţilor acestui sistem, şi pe baza lor să se modifice sistemul pentru o siguranţă mai mare; să se implementeze noul sistem.

Tema 2

Fie sistemul (P, C, K, e, d) unde:

- P va fi textul iniţial care trebuie criptat. Textul ar trebui să fie dat sub formă de biţi, dacă însă acesta este compus din cuvinte formate din caractere ce aparţin mulţimii $\{a, b, c, \dots z\}$ textul va fi transformat în biţi înaintea aplicării criptării.

- C va fi textul criptat ce va fi returnat sub formă de biţi. Dacă se doreşte se poate afişa în caractere ce aparţin mulţimii $\{a, b, c, \ldots z\}$.
- K va fi cheia dată cu care se va face criptarea. Dacă aceasta nu este dată sub formă de biţi, i se va face mai întâi transformarea binară. Lungimea cheii trebuie neapărat să fie egală cu lungimea textului care trebuie criptat.
- e este funcţia de criptare $P \times (T, K) \rightarrow C$ unde $e(P, K) = P\ xor\ K = (P + K) mod\ 2 = C$
- d este funcţia de decriptare $C \times (T, K) \rightarrow P$ unde $d(C, K) = C\ xor\ K = (C + K) mod\ 2 = P$.

Sistemul de mai sus este cunoscut sub numele de One Time Pad sau Sistemul Vernam.

Cerinţe:

1. Pornind de la acest sistem implementaţi un algoritm pentru el. Algoritmul trebuie să conţină funcţie de criptare, funcţie de decriptare, generator de chei pe baza unei parole.
2. Să se facă o criptanaliză pentru determinarea vulnerabilităţilor acestui sistem, şi pe baza lor să se modifice sistemul pentru o siguranţă mai mare; să se implementeze noul sistem.

Tema 3

Fie sistemul (P, C, K, e, d) unde:

- P este textul iniţial care tebuie criptat, fiind format din unul sau mai multe cuvinte alcătuite din litere ce aparţin mulţimii $\{a, b, c \ldots z\}$.
- C este textul ce se va obţine în urma criptării. Literele aparţin aceleiaşi mulţimi ca şi literele lui P.
- K este un cuvânt (sau un grup de litere fără înţeles) asupra caruia vor cădea de comun acord cei care vor să comunice. Cheia K de lungime n este formată din poziţiile literelor respective în alfabetul folosit $K = k_0 k_1 \ldots k_{n-1}$.
- e este funcţia de criptare definită astfel $P \times K \rightarrow C$ iar $e(p_i, k_r) = (p_i + k_r)(mod\ m) = C$ unde m este lungimea alfabetului folosit şi $r = i(mod\ n)$.
- d este funcţia de decriptare definită astfel $C \times K \rightarrow P$ şi $d(e(i), k_r) = (e(i) - k_r)(mod\ m)$ unde m este lungimea alfabetului folosit şi $r = i(mod\ n)$.

Sistemul de mai sus este cunoscut ca Sistemul Vigenere.

Cerinţe:

1. Pornind de la acest sistem implementaţi un algoritm pentru el. Algoritmul trebuie să conţină funcţie de criptare, funcţie de decriptare, generator de chei pe baza unei parole.

2. Să se facă o criptanaliză pentru determinarea vulnerabilităţilor acestui sistem, şi pe baza lor să se modifice sistemul pentru o siguranţă mai mare; să se implementeze noul sistem.

Tema 4

Fie un sistem care foloseşte cilindru Bazeries. Acest cilindru este format din aproximativ 20-30 de discuri numerotate, fiecare disc având la margine câte un alfabet diferit de restul alfabetelor de pe celelalte discuri, iar în mijloc au o gaură cu ajutorul careia acestea sunt prinse pe un ax. Discurile pot fi demontate şi montate într-o altă ordine pe ax.

După aranjarea discurilor, roţile pot fi rotite în orice direcţie până când mesajul care trebuie trimis este scris intr-un rând. Apoi, se copiază orice linie de pe roată în afară de cea pe care este scris mesajul rezultând astfel mesajul criptat. Cel ce primeşte mesajul trebuie să aranjeze discurile în ordinea corespunzătoare cheii, iar apoi, prin rotirea discurilor, să obţină mesajul criptat pe un rând. După obţinerea mesajului criptat se caută pe restul rândurilor mesajul iniţial.

Sistemul de mai sus este cunoscut sub numele de Sistemul Thomas Jefferson.

Cerinţe:

1. Să se găsească valorile (P, C, K, e, d) pentru acest sistem şi să se implementeze algoritmul.

2. Să se facă o criptanaliză pentru determinarea vulnerabilităţilor acestui sistem, şi pe baza lor să se modifice sistemul pentru o siguranţă mai mare; să se implementeze noul sistem.

Proiect 2

Tema 1

Fie sistemul (P, C, K, e, d) unde:

- P este textul iniţial care tebuie criptat, fiind format din unul sau mai multe cuvinte alcătuite din litere ce aparţin mulţimii $\{a, b, c \dots z\}$.
- C este textul ce se va obţine în urma criptării. Literele aparţin aceleiaşi mulţimi ca şi literele lui P.
- K este cheia secretă cu care se va face criptarea. K va fi format dintr-o pereche de două numere (a, b) unde a şi m sunt prime între ele (m este lungimea alfabetului folosit).
- e este funcţia de criptare definită astfel $P \times K \to C$ iar $e(P, K) = (aP+b)(mod\ m) = C$ unde m este lungimea alfabetului folosit.
- d este funcţia de decriptare definită astfel $C \times K \to P$ şi $d(C, K) = e^{-1}(C, K) = (a^{-1}(P - b))(mod\ m) = P$ unde m este lungimea alfabetului folosit şi a^{-1} este simetricul lui a în Z_{26}.

Sistemul de mai sus este cunoscut ca Sistemul Afin.

Cerinţe:

1. Pornind de la acest sistem implementaţi un algoritm pentru el. Algoritmul trebuie să conţină funcţie de criptare, funcţie de decriptare, generator de chei pe baza unei parole.
2. Să se facă o criptanaliză pentru determinarea vulnerabilităţilor acestui sistem, şi pe baza lor să se modifice sistemul pentru o siguranţă mai mare; să se implementeze noul sistem.

Tema 2

Fie sistemul (P, C, K, e, d) unde:

- P va fi textul iniţial care trebuie criptat. El este compus din cuvinte formate din caractere ce aparţin mulţimii $\{a, b, c, \ldots z\}$.
- C va fi textul criptat format, deasemenea, din caractere ce aparţin mulţimii $\{a, b, c, \ldots z\}$.
- K va fi cheia dată cu care se va face criptarea. În această metodă cheia este formată dintr-o matrice pătratică A_{mm} şi un vector B_m.
- e este funcţia de criptare $P \times K \to C$ unde $e(P, K) = C = AP + B(mod\ n)$
- d este funcţia de decriptare $C \times K \to P$ unde $d(C, K) = P = A^{-1}(C - B)(mod\ n)$.

Sistemul de mai sus este cunoscut sub numele de Codul Hill.

Cerinţe:

1. Pornind de la acest sistem implementaţi un algoritm pentru el. Algoritmul trebuie să conţină funcţie de criptare, funcţie de decriptare, generator de chei pe baza unei parole.
2. Să se facă o criptanaliză pentru determinarea vulnerabilităţilor acestui sistem, şi pe baza lor să se modifice sistemul pentru o siguranţă mai mare; să se implementeze noul sistem.

Proiect 3

Pornind de la algoritmul SEAL prezentat în curs rezolvaţi cerinţele:

1. Să se implementeze algoritmul.
2. Să se facă o criptanaliză pentru determinarea vulnerabilităţilor acestui sistem, şi pe baza lor să se modifice sistemul pentru o siguranţă mai mare; să se implementeze noul sistem.

Proiect 4

Tema 1

Să se implementeze un generator pseudo-aleator.

Tema 2

Să se implementeze Generatorul Shrinking bazat pe combinarea non-liniară a LFSR-urilor.

Proiect 5

Tema 1

Să se implementeze Algoritmul Berlekamp-Massey pentru testarea complexităţii liniare a unei secvenţe binare.

Tema 2

Să se scrie o lucrare despre obţinerea unor generatoare prin combinarea LFSR-urilor. Lucrarea trebuie să conţină:

- descrierea LFSR-urilor.
- algoritmi de combinare a LFSR-urilor.
- criptanaliza algoritmilor de combinare descrişi.
- un algoritm original de combinare a LFSR-urilor.
- criptanaliza algoritmului original.

Proiect 6

Tema 1

Să se scrie o lucrare care să facă o comparaţie amănunţită între DLP şi ECDLP. Să se compare şi eficacitatea acestora în criptografie.

Tema 2

Să se implementeze un algoritm pentru rezolvarea DLP pentru numere mici. Să se determine complexitatea acestuia şi să se analizeze care este lungimea maximă a numerelor pentru care poate fi folosit algoritmul.

Proiect 7

Tema 1

Să se scrie o lucrare care să facă o comparaţie amănunţită între DLP şi ECDLP. Să se compare şi eficacitatea acestora în criptografie.

Tema 2

Să se implementeze un algoritm pentru rezolvarea ECDLP pentru numere mici. Să se determine complexitatea acestuia şi să se analizeze care este lungimea maximă a numerelor pentru care poate fi folosit algoritmul.

Proiect 8

Fie sistemul (P, C, K, e, d) unde:

- P va fi textul iniţial care trebuie transmis. Ca şi la ceilalţi algoritmi el este compus din cuvinte formate din caractere ce aparţin mulţimii $\{a, b, c, \ldots z\}$.
- C va fi textul criptat format, deasemenea, din caractere ce aparţin mulţimii $\{a, b, c, \ldots z\}$.
- K reprezintă perechile de chei . O pereche de chei are trei componente: modulul n, componenta cheii publice e şi componenta cheii secrete d. Astfel cu cheia (e, n) se va face criptarea, iar cu cheia secretă (d, n) se va decripta. Pentru aflarea unei perechi de chei trebuie urmaţi mai mulţi paşi:
  1. Se generează două numere mari prime p şi q şi se calculează produsul acestora $n = pq$. n este făcut public dar nu şi p şi q; n ar trebui sa aibe cel puţin 1024 biţi.
  2. Se calculează $\Phi = (p-1)(q-1)$ şi se alege un număr întreg $e < n$ şi $(e, \Phi) = 1$. Deasemenea e se poate face public.
  3. Se alege un număr întreg d astfel încât $d * e \equiv 1 mod\ \Phi$. Numărul d nu se face public.
- en este funcţia de criptare definită astfel $P \times (e, n) \rightarrow C$. Mesajul criptat va fi $en(P, (e, n)) = p^e (mod\ n) = C$.
- de este funcţia cu care se face decriptarea $C \times (d, n) \rightarrow P$. Mesajul decriptat va fi $de(C, (d, n)) = c^d (mod\ n) = P$.

Sistemul de mai sus este cunoscut sub numele de RSA.

Cerinţe:

1. Pornind de la acest sistem implementaţi un algoritm pentru el. Algoritmul trebuie să conţină funcţie de criptare, funcţie de decriptare, generator de chei pe baza unei parole.
2. Să se facă o criptanaliză pentru determinarea vulnerabilităţilor acestui sistem, şi pe baza lor să se modifice sistemul pentru o siguranţă mai mare; să se implementeze noul sistem.

Proiect 9

Cunoaştem schema generală a unei semnături digitale:

- un algoritm pentru generarea cheilor care selectează o cheie privată la întâmplare dintr-un set de chei private. Algoritmul întoarce o cheie privată şi o cheie publică corespunzătoare.
- un algoritm de semnare care, dându-se un mesaj şi o cheie privată, va întoarce o semnătură.
- un algoritm pentru verificarea semnăturei care, dându-se o cheie publică şi o semnătură, va accepta sau va respinge semnătura.

Cerinţă:

Pornind de la schema de mai sus să se implementeze o schemă de semnătură oarbă.

Proiect 10

Cunoaştem următoarea schemă de semnătură digitală:

- Generarea cheii
  - se alege un întreg oarecare $x \in [0, r-1]$ unde r este ordinul grupului şi este prim.
  - cheia privată este x.
  - cheia publică este g^x unde g este generatorul grupului.
- Semnarea
  - se aplică mesajului m o funcţie hash H rezultând $h = H(m)$.
  - semnătura va fi $s = h^x$
- Verificarea
  - avem s, cheia publică g^x şi e funcţia de asociere.
  - se verifică dacă $e(s, g) = s(h, g^x)$

Schema descrisă mai sus este cunoscută ca Semnătura BLS.

Cerinţe:

1. Să se implementeze algoritmul.
2. Să se implementeze un algoritm de criptare la alegere în care autentificarea să se facă folosind semnătura BLS.

Proiect 11

Cunoaştem următoarea schemă de semnătură digitală:

- Generarea cheii
  - se alege un întreg oarecare $x \in [0, p-1]$ unde p este ordinul grupului şi este prim.
  - cheia privată este x.
  - cheia publică este $y = g^x mod\ p$ unde g este generatorul grupului.
- Semnarea
  - se aplică mesajului m o funcţie hash H rezultând $h = H(m)$.
  - semnătura va fi
    $$r = (g^k mod\ p) mod\ q$$
    $$s = (k^{-1}(h + xr)) mod\ q$$
    unde q este un divizor prim al lui $p-1$ şi k este un număr oarecare pozitiv mai mic decât q.
  - semnătura este (r, s).
- Verificarea
  - Fie m', r', s' versiunile primite ale lui m, r şi respectiv s, iar y este cheia publică a lui Alice.
  - se verifică mai întâi dacă $0 < r' < q$ şi $0 < s' < q$, dacă relaţiile sunt false semnătura este respinsă.
  - dacă acestea sunt îndeplinite atunci se va calcula:
    $$w = (s')^{-1} mod\ q$$
    $$u1 = (H(m')w) mod\ q$$
    $$u2 = ((r')w) mod\ q$$
    $$v = ((g^{u1} y^{u2}) mod\ p) mod\ q$$
  - dacă $v = r'$ atunci semnătura este validă.

Schema descrisă mai sus este cunoscută ca DSS.

Cerinţe:

1. Să se implementeze algoritmul.
2. Să se implementeze un algoritm de criptare la alegere în care autentificarea să se facă folosind DSS.

Proiect 12

Cunoaştem următoarea schemă de semnătură digitală:

- Generarea Cheilor
  1. Se alege un număr mare prim p astfel încât $p-1$ are un factor prim mare şi o rădăcină primitivă $g \in Z_p^*$;
  2. Se alege un număr oarecare x astfel încât $0 \leq x \leq p-2$;
  3. Se calculează $y = g^x (mod\ p)$;
  4. Cheia publică va fi (p, g, y) şi cheia secretă (p, g, x).
- Semnarea
  1. Se alege un k oarecare astfel încât $1 \leq k \leq p-2$ şi $cmmdc(k, p-1) = 1$;
  2. Se calculează $r = g^k (mod\ p)$ şi $s = k^{-1}(m - xr) mod (p-1)$, unde m este valoarea hash a mesajului iniţial;
  3. Semnătura este (r, s).
- Verificarea
  1. Se calculează $v = y^r r^s = (g^x)^r (g^k)^s mod\ p$;
  2. Se calculează $w = g^m mod\ p$;
  3. Semnătura este validă dacă este îndeplinită condiţia $v = w (mod\ p)$.

Schema descrisă mai sus este cunoscută ca Schema de Semnătură ElGamal.

Cerinţe:

1. Să se implementeze algoritmul.
2. Să se implementeze un algoritm de criptare la alegere în care autentificarea să se facă folosind Schema de Semnătură ElGamal.

Proiect 13

Cunoaştem următoarea schemă de semnătură digitală:

- Generarea Cheilor
  1. Se alege un grup de ordin q cu generatorul g, şi o funcţie hash H.
  2. Se alege un număr oarecare x astfel încât $0 \leq x \leq q$ care va fi cheia secretă;
  3. Se calculează $y = g^x$ care va fi cheia publică;
- Semnarea
  1. Se alege un k oarecare;
  2. Se calculează
  $$r = g^k (mod\ p)$$
  $$e = H(M||r)$$
  $$s = (k - xe)(mod\ q)$$
  3. Semnătura este (e, s).
- Verificarea
  1. Se calculează
  $$r_v = g^s y^e$$
  $$e_v = H(M||r_v)$$
  2. Dacă $e_v = e$ atunci semnătura este validă.

Schema descrisă mai sus este cunoscută ca Schema de Semnătură Schnorr.

Cerinţe:

1. Să se implementeze algoritmul.
2. Să se implementeze un algoritm de criptare la alegere în care autentificarea să se facă folosind Schema de Semnătură Schnorr.

Proiect 14

Tema 1

Să se scrie o lucrare despre funcţiile hash. Lucrarea trebuie să conţină:

- definirea funcţiilor hash.
- descrierea funcţiilor hash importante.
- algoritmii funcţiilor hash descrise.
- criptanaliza funcţiilor hash descrise.
- compararea funcţiilor descrise din punct de vedere criptografic.
- aducerea unei contribuţii originale în domeniu.

Tema 2

Să se implementeze un algoritm pentru funcţia hash RIPEMD-160.

Proiect 15

Tema 1

Să se implementeze un algoritm pentru una din funcţiile hash SHA.

Tema 2

Să se implementeze un algoritm pentru funcţia hash MD5.

Proiect 16

Fie protocolul:

1. Cei doi care vor să comunice stabilesc două numere întregi prime p şi m iar $1 < m < p-1$. Numărul p ar trebui să aibe cel puţin 1024 biţi. Nu contează dacă aceste două numere se află, nu trebuie sa fie neapărat secrete.

2. Apoi prima persoană îşi alege un număr secret x unde $1 < x < p-1$ şi a doua persoană un alt număr secret y unde $1 < y < p-1$ iar x şi y nu au nici un divizor comun cu $p-1$.

3. Prima persoană calculează $m^x mod\ p$ şi rezultatul îl comunică celei de-a doua persoană. A doua persoană procedează la fel cu numărul său secret $m^y mod\ p$.

4. Fiecare persoană înmulţeşte rezultatul primit de la cealaltă persoană cu numărul său secret. Astfel:
$$K = (m^x)^y = m^{xy} = (m^y)^x mod\ p$$

După executarea paşilor de mai sus cheia K va reprezenta cheia comună. Protocolul descris este cunoscut sub numele de Diffie-Hellman.

Cerinţe:

1. Să se implementeze algoritmul pentru acest protocol.

2. Să se scrie o lucrare pornind de la protocol Diffie-Hellman. Lucrarea va conţine:

   - descrierea protocolului.
   - importanţa acestuia în criptografie.
   - criptanaliza protocolului.
   - descrierea unui protocol original plecând de la aceasta.
   - compararea protocolului original cu Diffie-Hellman din punct de vedere al vulnerabilităţilor.

Proiect 17

Considerăm p un număr suficient de mare pentru a fi infeasibil calculul logaritmului în $\mathbb{Z}_p^*$ şi fie g un generator pentru $\mathbb{Z}_p^*$. De asemenea fiecare utilizator va dispune de un set de chei publice/private (s_A, v_A) pentru a fi utilizate cu o schemă de semnătură digitală. Fie protocolul:

1. Alice alege aleator a, $0 \leq a \leq p-2$
2. Alice calculează $c = g^a$ şi trimite lui Bob rezultatul c
3. Bob alege aleator b, $0 \leq b \leq p-2$
4. Bob calculează cheia secretă $k = g^{ab}$ şi semnează concatenarea $g^a \mid\mid g^b$ cu cheia lui privată $s = Sign_{s_B}(g^a \mid\mid g^b)$ şi trimite $(g^b, E_k(b))$ lui Alice.
5. Alice calculează cheia secretă $k = g^{ab}$, decriptează semnătura s şi o verifică. Dacă verificările nu eşuează atunci Alice este convinsă că Bob este cel cu care comunică. Alice va genera apoi semnătura $s = Sign_{s_A}(g^a \mid\mid g^b)$ şi trimite $E_k(s)$ lui Bob
6. Bob decriptează $E_k(s)$ şi verifică semnătura lui Alice. Dacă verificările nu eşuează Bob a stabilit cu Alice cheia de sesiune $k = g^{ab}$

Protocolul de mai sus este cunoscut sub numele de Station-to-Station.

Cerinţe:

1. Să se implementeze algoritmul pentru acest protocol folosind o schemă de semnătură digitală la alegere.
2. Să se scrie o lucrare pornind de la protocolul Station-to-Station. Lucrarea va conţine:
   - descrierea protocolului.
   - importanţa acestuia în criptografie.
   - criptanaliza protocolului.
   - analizarea protocolului prin aplicarea succesivă a mai multor scheme de semnătură digitală.

Proiect 18

Fie protocolul:

1. Alice alege $r \in \mathbb{Z}^*$ aleator
2. Alice calculează $a = r^2$ şi trimite a lui Bob
3. Bob alege aleator $e \in \{0, 1\}$ şi trimite e lui Alice
4. Alice calculează $b = ry^e$ şi trimite b lui Bob
5. Dacă $b = ax^e$ atunci Bob acceptă dovada lui Alice

Protocolul de mai sus este un protocol pentru dovedirea identităţii cunoscută sub numele de Schema Fiat-Shamir simplificată.

Cerinţe:

1. Să se implementeze algoritmul pentru acest protocol.
2. Să se scrie o lucrare pornind de la protocolul pentru dovedirea identităţii cunoscută sub numele de Schema Fiat-Shamir simplificată. Lucrarea va conţine:
   - descrierea noţiunii de protocol pentru dovedirea identităţii.
   - descrierea protocolului Fiat-Shamir.
   - importanţa acestuia în criptografie.
   - criptanaliza protocolului.
   - descrierea unui protocol original pornind de la acesta.
   - comparaţia celor două protocoale din punct de vedere criptografic.

Proiect 19

Tema 1

Să se scrie o lucrare despre protejarea sistemelor împotriva malware. Lucrarea va conţine:

- descrierea noţiunii de malware.
- descrierea fiecărui tip de malware.
- exemple de malware şi efectele provocate de aceştia.
- protejarea sistemelor împotriva malware.
- descrierea unor soft-uri antivirus/antispy şi modul de funcţionare al acestora.
- comparaţia soft-urilor descrise.

Tema 2

Să se implementeze un soft malware.

Proiect 20

Tema 1

Să se scrie o lucrare despre protocoalele criptografice. Lucrarea va conţine:

- descrierea protocoaleleor de autentificare.
- descrierea protocoaleleor de schimb de chei.
- descrierea protocoaleleor pentru dovedirea identităţii.
- descrierea a cel puţin un protocol din fiecare.
- criptanaliza protocoalelor descrise.
- comparaţia celor trei tipuri de protocoale şi combinarea acestora din punct de vedere criptografic.
- descrierea unui protocol original plecând de la cele descrise.

Tema 2

Să se scrie o lucrare despre securitate Internet. Lucrarea va conţine:

- securitatea reţelelor.
- descrierea vulnerabilităţilor reţelelor.
- securitatea Internet.
- securitatea e-mailurilor.
- protoacoale folosite pentru asigurarea securităţii.

Tema 3

Să se scrie o lucrare despre Online Banking. Lucrarea va conţine:

- descrierea câtorva protocoale importante.
- descrierea vulnerabilităţilor acestor protocoale.

- compararea acestor protocoale.
- descrierea unui protocol original.
- compararea protocolului original cu cele existente deja.