Proiecte

23 februarie 2012

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

- P va fi textul inițial care trebuie criptat. El este compus din cuvinte formate din caractere ce aparțin mulțimii $\{a, b, c, \ldots z\}$.
- C va fi rezultatul obținut în urma criptării lui P. Se observă că textul C va fi și el format din caractere din mulțimea $\{a, b, c, \ldots z\}$.
- K va fi cheia dată cu care se va face criptarea. Cheia poate fi un cuvânt cu ajutorul căruia se va alcătui pătratul Playfair sau se poate da direct pătratul. Dacă, cheia este un cuvânt în care se repetă litere acestea se scriu doar o singură dată (de exemplu: Tomorrow va deveni Tomrw).
- e este funcția de criptare $P \times K \to C$ $e(P, K) = C$. Mai jos sunt regulile de criptare pentru o pereche de litere (x, y):
  1. Dacă cele două litere sunt în colțurile opuse ale unui dreptunghi literele rezultate în urma criptării vor fi cele două litere aflate in colțurile respectiv opuse (în cazul criptării cu sistemul Playfair dublu literele se vor lua din colțurile de pe aceeași coloană).
  2. Dacă cele două litere sunt pe aceeași coloană se vor lua literele de sub ele (se presupune că linia 1 este sub linia 5).
  3. Dacă cele două litere sunt pe aceeași linie se vor lua literele din dreapta lor (se presupune că prima coloană este la dreapta coloanei 5).
  4. Dacă cele două litere sunt identice se introduce o literă între ele (acest lucru nu este valabil în cazul folosirii a două pătrate Playfair deoarece literele sunt în pătrate diferite).
  5. Dacă la sfârșit rămâne doar o literă se mai adaugă una pentru a putea forma o pereche.
- d este funcția de decriptare $C \times K \to P$ adică $d(C, K) = P$. Decriptarea pentru o pereche de două litere:
  1. Dacă cele două litere sunt în colțurile opuse ale unui dreptunghi literele rezultate în urma decriptării vor fi cele două litere aflate in colțurile respectiv opuse (în cazul decriptării cu sistemul Playfair dublu literele se vor lua din colțurile de pe aceeași coloană).
  2. Dacă cele două litere sunt pe aceeași coloană se vor lua literele de deasupra lor (se presupune că linia 5 este deasupra liniei 1).
  3. Dacă cele două litere sunt pe aceeași linie se vor lua literele din stânga lor (se presupune că a 5-a coloană este la stânga coloanei 1).

Sistemul de mai sus este cunoscut ca Sistemul Playfair.
1. Pornind de la acest sistem implementați un algoritm pentru el. Algoritmul trebuie să conțină funcție de criptare, funcție de decriptare, generator de chei pe baza unei parole.
2. Să se facă o criptanaliză pentru determinarea vulnerabilităților acestui sistem, și pe baza lor să se modifice sistemul pentru o siguranță mai mare; să se implementeze noul sistem.

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

- P va fi textul inițial care trebuie criptat. El este compus din cuvinte formate din caractere ce aparțin mulțimii $\{a, b, c, \ldots z\}$.
- C va fi textul criptat format, deasemenea, din caractere ce aparțin mulțimii $\{a, b, c, \ldots z\}$.
- K va fi cheia dată cu care se va face criptarea. În această metodă cheia este formată dintr-o matrice pătratică T_{77} și un cuvânt K. Matricea are pe $t_{00} = 0$, prima linie de la elementul t_{01} până la elementul t_{06} va avea ADFGVX. La fel va fi și pe prima coloană de la elementul t_{10} până la elementul t_{60}. În rest matricea va avea toate literele alfabetului englez la care se adaugă numerele de la 1 la 10 (rămân 36 de elemente necompletate, alfabetul are 26 de litere, deci vor rămâne 10 elemente ce vor fi numere). K va fi un cuvânt (în care literele ce se repetă se trec doar o singură dată) sau un grup de litere.
- e este funcția de criptare $P \times (T, K) \to C$ unde $e(P, (T, K)) = C$
- d este funcția de decriptare $C \times (T, K) \to P$ unde $d(C, (T, K)) = P$.

Sistemul de mai sus este cunoscut ca Sistemul ADFGVX.
3. Pornind de la acest sistem implementați un algoritm pentru el. Algoritmul trebuie să conțină funcție de criptare, funcție de decriptare, generator de chei pe baza unei parole.
4. Să se facă o criptanaliză pentru determinarea vulnerabilităților acestui sistem, și pe baza lor să se modifice sistemul pentru o siguranță mai mare; să se implementeze noul sistem.

5. Un sistem criptografic este descris de următorii pași:

   1. segmentul inițial de 64 de biți este supus unei permutări (IP).
   2. rezultatul obținut în urma permutării se va împărți în două blocuri de câte 32 de biți, notați L (left) și R (right).
   3. 48 de biți ai cheii K sunt combinați cu un R "expandat" la 48 de biți (16 biți din R se vor repeta) printr-o funcție non-liniară, iar rezultatul obținut se va reduce la un string de 32 de biți (notat cu X).
   4. L va fi înlocuit cu R iar R va fi înlocuit cu X *xor* L rezultând un nou R de 32 de biți.
   5. se vor repeta cei doi pași anteriori de 16 ori, folosind la pasul 3 un alt segment de 48 de biți al lui K.
   6. celor 64 de biți obținuți în final li se va aplica inversa permutării inițiale (IP^{-1}) rezultând textul criptat.

Sistemul de mai sus este cunoscut ca Sistemul DES.
5. Pornind de la acești pași implementați un algoritm pentru sistemul DES. Algoritmul trebuie să conțină funcție de criptare, funcție de decriptare, generator de chei pe baza unei parole.
6. Să se facă o criptanaliză pentru determinarea vulnerabilităților acestui sistem, și pe baza lor să se propună modificări asupra sistemul pentru o siguranță mai mare.
7. Să se implementeze un algoritm pentru 3DES prin aplicarea sistemului DES de trei ori.
8. Să se scrie o lucrare despre sistemul DES. Lucrarea să conțină:

   - descrierea sistemului DES.
   - descrierea sistemului 3DES.
   - criptanaliza sistemului DES.
   - criptanaliza sistemului 3DES.
   - compararea celor două sisteme din punct de vedere criptografic.

9. Având cei trei algoritmi (prezentați și în curs) pentru sistemul AES, să se implementeze acest sistem.

Algorithm 49 AES CIPHER.Criptare

aesCriptare

1. **Start**
2. Se dă in o matrice
3. $s \leftarrow in$
4. $s \leftarrow AddRoundKey(s, w[0, N_b - 1])$
5. **for** r to $N_r - 1$ **do**
   - 5.1 $s \leftarrow SubBytes(s)$
   - 5.2 $s \leftarrow ShiftRows(s)$
   - 5.3 $s \leftarrow MixedColumns(s)$
   - 5.4 $s \leftarrow AddRoundKey(s, w[rN_b, (r+1)N_{b-1}])$
6. $s \leftarrow SubBytes(s)$
7. $s \leftarrow ShiftRows(s)$
8. $s \leftarrow AddRoundKey(s, w[N_rN_b, (N_r+1)N_b - 1])$
9. $out \leftarrow s$
10. Textul criptat este out

Algorithm 50 AES CIPHER.Decriptare

aesDecriptare

1. **Start**
2. Se dă in o matrice
3. $s \leftarrow in$
4. $s \leftarrow AddRoundKey(s, w[N_r, (N_r+1)N_b - 1])$
5. **for** r to $N_r - 1$ **do**
   - 5.1 $s \leftarrow InvShiftRows(s)$
   - 5.2 $s \leftarrow InvSubBytes(s)$
   - 5.3 $s \leftarrow AddRoundKey(s, w[rN_b, (r+1)N_{b-1}])$
   - 5.4 $s \leftarrow InvMixedColumns(s)$
6. $s \leftarrow InvShiftRows(s)$
7. $s \leftarrow InvSubBytes(s)$
8. $s \leftarrow AddRoundKey(s, w[0, N_b - 1])$
9. $out \leftarrow s$
10. Textul decriptat este out

Algorithm 51 AES CIPHER.Generare chei

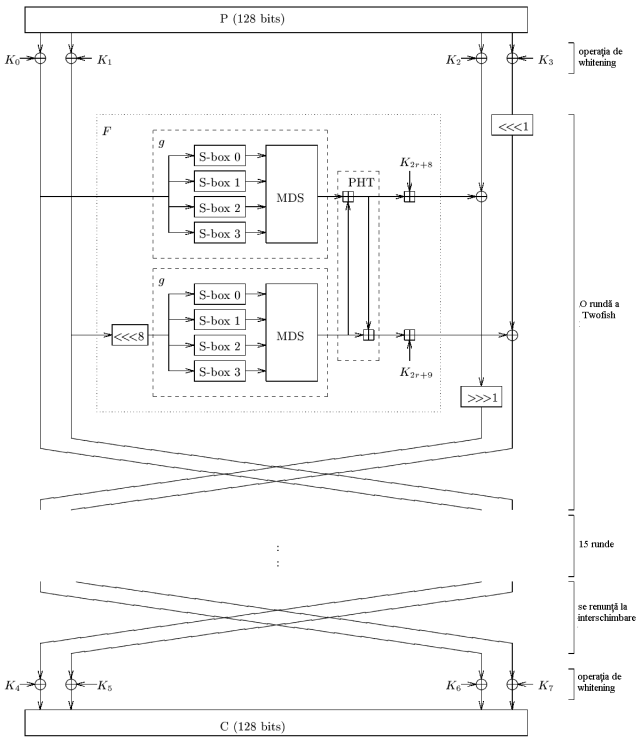
aesGenerare

1. Start
2. Se dă k
3. $Rcon[1] \leftarrow 0x01000000$
4. $Rcon[2] \leftarrow 0x02000000$
5. $Rcon[3] \leftarrow 0x04000000$
6. $Rcon[4] \leftarrow 0x08000000$
7. $Rcon[5] \leftarrow 0x10000000$
8. $Rcon[6] \leftarrow 0x20000000$
9. $Rcon[7] \leftarrow 0x40000000$
10. $Rcon[8] \leftarrow 0x80000000$
11. $Rcon[10] \leftarrow 0x36000000$
12. **for** $i = 0$ to $(N_k - 1)$ do
    - 12.1 $w[i] \leftarrow [k_{4i}, k_{4i+1}, k_{4i+2}, k_{4i+3}]$
13. **for** $i = N_k$ to $(N_b(N_r + 1) - 1)$ do
    - 13.1 $t \leftarrow w[i-1]$
    - 13.2 **if** $(i \bmod N_k = 0)$ **then**
      - 13.2.1 $t \leftarrow SubWord(RotWord(t))$ xor $RCon[i/N_k$
    - 13.3 **elseif** $(N_k > 6) \& \& (i \bmod N_k = 4)$ **then**
      - 13.3.1 $t \leftarrow SubWord(t)$
14. $w[i] \leftarrow w[i - N_k]$ xor t
15. Cheia folosită este w

10. Să se scrie o lucrare care să conțină:

- descrierea sistemului AES.
- criptanaliza sistemului AES.
- compararea din punct de vedere criptografic acestui sistem cu cele dinaintea lui.

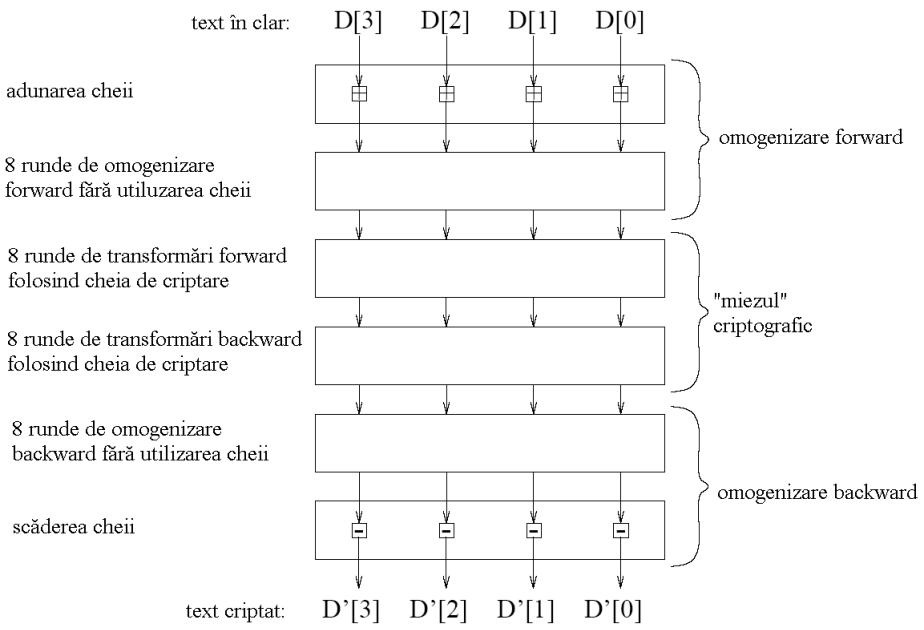
Se dă schema:



Sistemul de mai sus este cunoscut sub numele de Sistemul Twofish. Acesta este un algoritm care acceptă dimensiuni variabile ale cheii de criptare de până la *256* biți. Cifrul în sine este o rețea *Feistel* cu *16* runde de criptare care folosește o funcție bijectivă F compusă din *4* S-boxuri de dimensiune 8×8 biți, o matrice *MDS* de dimensiune 4×4 peste spațiul $GF(2^8)$, o transformare pseudo-*Hadamard*, rotații pe biți și un algoritm de programare a cheii.

11. Plecând de la cele descrise mai sus, să se implementeze algoritmul sistemului. Acesta să conțină o funcție de criptare, una de decriptare și una de generare a cheilor.

Se dă schema:



Sistemul de mai sus este cunoscut sub numele de MARS. Notațiile din schema de mai sus sunt:

- D[] este un șir de 4 de cuvinte a 32 biți. Inițial D conține cuvintele textului în clar, iar la finalul procesului de criptare va conține cuvintele criptate.
- K[] este un șir de 40 de cuvinte a 32 biți care reprezintă cheia de criptare expandată.
- S[] este S-boxul ce conține cele 512 cuvinte a 32 biți. În unele cazuri acest S-box va fi considerat ca fiind compus din 2 S-boxuri a câte 256 cuvinte fiecare.

12. Plecând de la cele schema de mai sus, să se implementeze algoritmul sistemului. Acesta să conțină o funcție de criptare, una de decriptare și una de generare a cheilor.

Un sistem criptografic este descris de următorii pași:

- o permutare inițială.
- 32 de runde fiecare constând într-o operație de omogenizare folosind o cheie a rundei, o substituție bazată pe S-boxuri și o transformare liniară, care este omisă în ultima rundă și înlocuită cu o operație de omogenizare bazată pe o cheie.
- o permutare finală.

Pașii de mai sus descriu sistemul Serpent.
13. Plecând de la cele descrise mai sus, să se implementeze acest sistem. Acesta să conțină o funcție de criptare, una de decriptare și una de generare a cheilor.

14. Având cei trei algoritmi (prezentați și în curs) pentru sistemul RC6, să se implementeze acest sistem.

Algorithm 21 Algoritmul. RC6 Criptare

criptare_rc6$((A,B,C,D),r,w,S)$

1. *Start*
2. *B= B+S[0]*
3. *D= D+S[1]*
4. *for i=1 to r do*
   - 4.1. $t = (B \times (2B+1)) \lll lg\ w$
   - 4.2. $u = (D \times (2D+1)) \lll lg\ w$
   - 4.3. $A = ((A \oplus t) \lll u) + S[2i]$
   - 4.4. $C = ((C \oplus u) \lll t) + S[2i+1]$
   - 4.5. $(A,B,C,D) \leftarrow (B,C,D,A)$
5. *A=A+S[2r+2]*

Algorithm 22 Algoritmul RC6. Decriptare

decripare_rc6$((A,B,C,D),r,w,S)$

1. *Start*
2. $C = C - S[2r+3]$
3. $A = A - S[2r+2]$
4. *for i = r downto 1 do*
   - 4.1 $(A,B,C,D) \leftarrow (D,A,B,C)$
   - 4.2 $u = (D \times (2D+1)) \lll lg\ w$
   - 4.3 $t = (B \times (2B+1)) \lll lg\ w$
   - 4.4 $C = ((C - S[2i+1]) \ggg t) \oplus u$
   - 4.5 $A = ((A - S[2i]) \ggg u) \oplus t$
5. $D = D - S[1]$
6. $B = B - S[0]$

Algorithm 23 Algoritmul RC6. Programarea cheii

programare_cheie(L,R)

1. *Start*
2. $S[0] = P_w$
3. *for i=1 to 2r+3 do*
   - 3.1 $S[i] = S[i-1] + Q_w$
4. $A = B = i = j = 0$
5. $v = 3 \times max\{c, 2r+4\}$
6. *for* $s = 1$ *to* v *do*
   - 6.1 A= S[i]= (S[i]+A+B) $\lll$ 3
   - 6.2 B=L[j]=(L[j]+A+B) $\lll$ (A+B)
   - 6.3 i=(i+1) mod (2r+4)
   - 6.4 j=(j+1) mod c

Un sistem criptografic este descris de următoarea schemă:

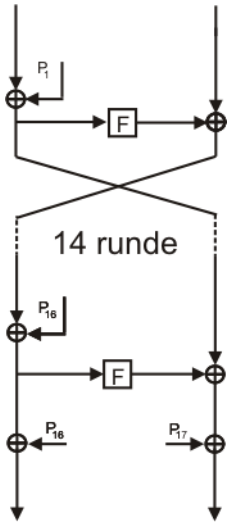


Figura 1: Blowfish

Sistemul de mai sus este cunoscut sub numele de Blowfish. Blowfish folosește chei cu lungimi între 32 și 448 de biți și S-boxes. În figura de mai sus este reprezentată acțiunea algoritmului. Fiecare linie reprezintă 32 de biți. Algoritmul păstrează două subchei: cele 18 șiruri P și cele patru S-box-urile. S-box-urile acceptă un input de 8 biți și produc un output de 32 de biți. O intrare a lui P este folosită la fiecare rundă, iar după runda finală fiecare jumătate din blocul de date este adunat modulo 2 cu una dintre cele două intrări nefolosite ale lui P care au rămas.
15. Pornind de la această schemă implementați un algoritm pentru acest sistem. Algoritmul trebuie să conțină funcție de criptare, funcție de decriptare, generator de chei.

Un sistem criptografic este descris de următoarea schemă:

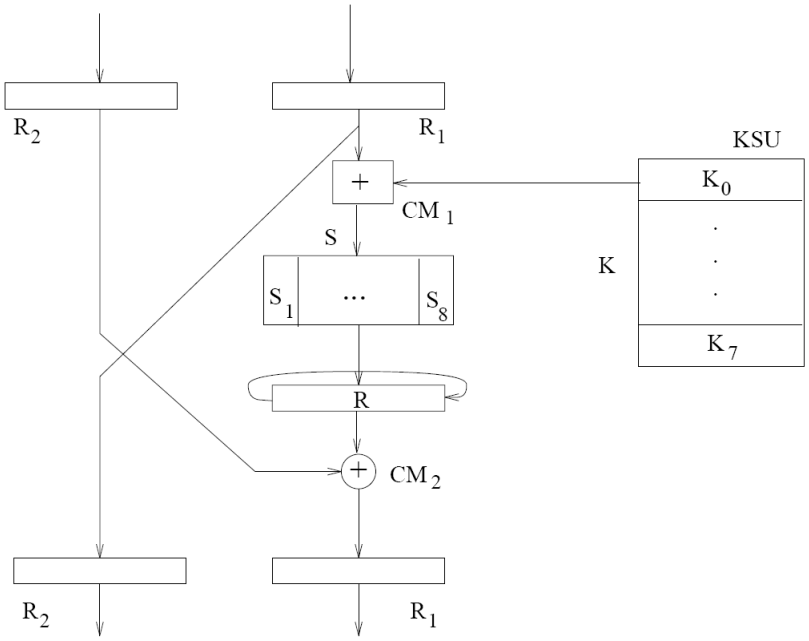


Figura 2: Structura generală a cifrului GOST

Sistemul de mai sus este cunoscut sub numele de GOST.
16. Pornind de la această schemă implementați un algoritm pentru acest sistem. Algoritmul trebuie să conțină funcție de criptare, funcție de decriptare, generator de chei.

17. Să se scrie o lucrare despre sistemele candidate pentru AES. Lucrarea va conține:

    - descrierea condițiilor impuse de NIST.
    - descrierea celor cinci sisteme finaliste.
    - criptanaliza și compararea acestor sisteme.
    - alegerea personală a câștigătorului și motivarea acesteia.

18. Plecând de la algoritmul de mai jos să se implementeze o cascadă Gollman pentru generarea cheilor.

Algorithm 10 Cascada Gollman

casGollman

1. *Start*
2. *for* $i = 1, 2 \ldots$ *do*
   - 2.1. *Shiftarea rundei 1 ;i producerea lui* $y_i^{(1)}$
   - 2.2. *for* $n = 2, \ldots N$ *do*
     - 2.2.1. *Shiftarea rundei* n *de* $y_i^{(n-1)}$ *ori şi producerea:*

$$y_i^{(n)} = y_i^{(n-1)} \oplus s^{(n)}_{\sigma_{n-1}(i)}$$

$$\sigma_{n-1}(i) = \sum_{k=1}^{i} y_i^{(k-1)}$$

     - 2.2.2 *Alternativ se poate shifta runda* n *de* $y_i^{(n-1)} + 1$ *ori.*
3. $z_i = y_i^N$
4. *return* $z_i \;\; i = 1, 2, \ldots$

Pașii unui protocol sunt:

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

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

3. Prima persoană calculează $m^x mod\ p$ și 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 înmulțește rezultatul primit de la cealaltă persoană cu numărul său secret. Astfel:

$$K = (m^x)^y = m^{xy} = (m^y)^x mod\ p$$

   unde K va fi cheia comună.

Protocolul de mai sus este cunoscut sub numele de Diffie-Hellman.
19. Plecând de la descrierea de mai sus, să se implementeze acest protocol.

Valorile sistemului (P, C, K, e, d) sunt:

- P va fi textul inițial care trebuie transmis. Ca și la ceilalți algoritmi el este compus din cuvinte formate din caractere ce aparțin mulțimii $\{a, b, c, \ldots z\}$.
- C va fi textul criptat format, deasemenea, din caractere ce aparțin mulțimii $\{a, b, c, \ldots z\}$.
- K reprezintă perechile de chei . Cheile vor fi obținute astfel:
  1. Se generează două numere mari prime p și q. Pentru un calcul mai simplu al rădăcinii se pot alege astfel încât $p = q = 3(mod\ 4)$.
  2. Se calculează $n = p * q$.
  3. n va fi cheia publică iar perechea (p, q) vor fi cheia privată.
- e este funcția de criptare definită astfel $P \times (n) \to C$. Mesajul criptat va fi $e(P, n) = p^2 (mod\ n) = C$.
- d este funcția cu care se face decriptarea $C \times (p, q) \to P$. Mesajul decriptat va fi $d(C, (p, q)) = P$. Operația de decriptare va avea patru rezultate corecte dintre care unul este textul căutat. Mai jos vom descrie pașii pentru decriptare:
  1. Se vor calcula rădăcinile:
  $$P_p = \sqrt{C}\ mod\ p$$
  $$P_q = \sqrt{C}\ mod\ q$$
  2. Prin algoritmul extins al lui Euclid vom avea y_p, y_q astfel încât:
  $$y_p * p + y_q * q = 1$$
  3. Cu ajutorul teoremei chinezești a resturilor vom calcula cele patru rădăcini ale lui C din care se va alege una ca fiind mesajul inițial:
  $$r = (y_p * p * P_q + y_p * q * P_p) mod\ n$$
  $$-r = n - e$$
  $$s = (y_p * p * P_q - y_p * q * P_p) mod\ n$$
  $$-s = n - s$$

Sistemul de mai sus este cunoscut sub numele de Sistemul Rabin.
20. Pornind de la acest sistem implementați un algoritm pentru el. Algoritmul trebuie să conțină funcție de criptare, funcție de decriptare, generator de chei.
21. Să se facă o criptanaliză pentru determinarea vulnerabilităților acestui sistem, și pe baza lor să se modifice sistemul pentru o siguranță mai mare; să se implementeze noul sistem.

Fie algoritmii:

- Algoritmul de Generare al Cheilor
  1. Se alege un număr mare prim p astfel încât $p-1$ are un factor prim mare și 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) și cheia secretă (p, g, x).
- Algoritmul de Criptare
  1. Se alege un k oarecare din Z_p^*;
  2. Se calculează $K = y^k (mod\ p)$;
  3. Se calculează:
  $$c_1 = g^k (mod\ p)$$
  $$c_2 = Km (mod\ p)$$
  4. (c_1, c_2) este textul criptat corespunzător mesajului m.
- Algoritmul de Decriptare
  1. Se calculează $K = c_1^x (mod\ p)$;
  2. Se calculează $m = c_2/K (mod\ p)$.
  Decriptarea mesajului se poate face și astfel:

$$x_1 = p - 1 - x$$

$$c_1^{x_1} c_2 = g^{kx_1} Km (mod\ p) = g^{k(p-1-x)} Km (mod\ p)$$
$$c_1^{x_1} c_2 = g^{k(p-1-x)} y^k m (mod\ p) = (g^{p-1})(g^x)^{-k} y^k m (mod\ p)$$
$$c_1^{x_1} c_2 = y^{-k} y^k m (mod\ p) = m (mod\ p)$$

Sistemul format din algoritmii de mai sus se numește Sistemul ElGamal.
22. Pornind de la acest sistem implementați un algoritm pentru el. Algoritmul trebuie să conțină funcție de criptare, funcție de decriptare, generator de chei.
23. Să se facă o criptanaliză pentru determinarea vulnerabilităților acestui sistem, și pe baza lor să se modifice sistemul pentru o siguranță mai mare; să se implementeze noul sistem.

Fie algoritmii:

- Algoritmul de Generare al Cheilor
  1. Alice generează două numere mari prime p și q astfel încât $p \neq q$ și $(p, q) \equiv 3 \ mod \ 4$.
  2. Alice calculează $N = pq$.
- Algoritmul de Criptare
  1. Bob codează mesajul m ca un string de L biți $(m_0, \ldots, m_{L-1})$.
  2. Bob alege un număr aleator r, unde $1 < r < N$, și calculează $x_0 = r^2 \ mod \ N$.
  3. Bob folosește un generator BBS pentru a genera L biți aleatori $(b_0, \ldots, b_{L-1})$ astfel:
     (a) Pentru $i = 0$ la $L - 1$ $b_i =$ cel mai nesemnificativ bit al luix_i
     (b) Se incrementează i
     (c) $x_i = (x_{i-1})^2 \ mod \ N$
  4. Bob calculează textul criptat astfel: $\vec{c} = \vec{m} \oplus \vec{b}, y = x_0^{2^L} \ mod \ N$.
  5. Bob trimite textul cirat $(c_0, \ldots, c_{L-1})$ și pe y.
- Algoritmul de Decriptare
  1. Alice calculează $r_p = y^{((p+1)/4)^L} \ mod \ p$ și $r_q = y^{((q+1)/4)^L} \ mod \ q$.
  2. Alice calculează sămânța inițială $x_0 = q(q^{-1} \ mod \ p)r_p + p(p^{-1} \ mod \ q)r_q \ mod \ N$
  3. Din x_0, recalculează $\vec{b}$ folosind un generator BBS, la fel ca în algoritmul de criptare.
  4. Calcularea textului în clar $\vec{m} = \vec{c} \oplus \vec{b}$.

Sistemul format din algoritmii de mai sus se numește Blum-Goldwasser.
23. Pornind de la acest sistem implementați un algoritm pentru el. Algoritmul trebuie să conțină funcție de criptare, funcție de decriptare, generator de chei.
24. Să se facă o criptanaliză pentru determinarea vulnerabilităților acestui sistem, și pe baza lor să se modifice sistemul pentru o siguranță mai mare; să se implementeze noul sistem.

Fie algoritmii:

- Algoritmul de Generare al Cheilor
  1. Alice generează două numere mari, prime, distincte alese aleator p și q.
  2. Alice calculează $N = pq$.
  3. Alice găsește un x astfel încât $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = -1$ adică $\left(\frac{x}{N}\right)$ să fie $+1$. Dacă $(p, q) = 3 \ mod \ 4$ atunci $N - 1$ are sigur proprietatea de menționată.
  4. Cheia publică este (x, N). Cheia privată este (p, q).
- Algoritmul de Criptare
  1. Bob criptează mesajul m ca un string de biți $(m_1, ..., m_n)$.
  2. Pentru fiecare bit m_i, Bob generează o valoare $y < N$. El calculează $c_i = y^2 x^{m_i} \ modN$.
  3. Bob trimite textul criptat $(c_1, \ldots, c_n)$.
- Algoritmul de Decriptare
  1. Pentru fiecare i, folosind cheia (p, q), Alice determină dacă valoarea c_i este un rest pătratic.
  2. Dacă da atunci $m_i = 0$, altfel $m_i = 1$.
  3. Mesajul decriptat este $(m_1, \ldots, m_n)$.

Sistemul format din algoritmii de mai sus se numește Goldwasser-Micali.
25. Pornind de la acest sistem implementați un algoritm pentru el. Algoritmul trebuie să conțină funcție de criptare, funcție de decriptare, generator de chei.
26. Să se facă o criptanaliză pentru determinarea vulnerabilităților acestui sistem, și pe baza lor să se modifice sistemul pentru o siguranță mai mare; să se implementeze noul sistem.

27. Să se scrie o lucrare descpre curbe eliptice și aplicarea lor în criptografie. Lucrarea va conține:

- descrierea matematică a curbelor eliptice.
- exemple de calcule asupra curbelor eliptice.
- condițiile de alegere a unei cube eliptice criptografice bune.
- exemple de sisteme care folosesc curbele eliptice.
- compararea sistemelor obișnuite cu cele care folosesc curbe eliptice din punct de vedere al securtății.

Avem ecuația generală a unei curbe $y^2 = x^3 + ax + b$ și dorim obținerea mesajului m ca punct al curbei $E(F_p)$ unde $p = 3(mod\ 4)$. Pentru a aplica această curbă unui mesaj trebuie urmați pașii:

1. Presupunem că mesajul m este un număr astfel încât $0 \neq m \neq \frac{p}{1000} - 1$
2. Se ia $x_j = 1000m + j$ unde $j = 0, 1, 2 \ldots, 999$
3. Se calculează $c_j = x_j^3 + ax_j + b$ până vom avea $c_j^{\frac{p-1}{2}} \equiv 1(mod\ p)$
4. Se calculează $y_j = \sqrt{c_j}$
5. Punctul obținut $P_m = (x_j, y_j) = (x_j, y_j^{(p+1)/4})$ este punctul corespunzător mesajului m

28. Să se implementeze un algoritm plecând de la pașii de mai sus.
29. Să se implementeze un algoritm pentru aplicarea unei curbe eliptice unui mesaj utilizând cifre pentru fiecare literă din alfabet pentru coordonata x, calculând y prin înlocuirea în ecuația curbei.
30. Să se scrie o lucrare despre metodele de aplicare a unei curbe eliptice asupra unui mesaj. Lucrarea va conține:

- descrierea matematică a curbelor eliptice.
- descrierea metodelor existente de aplicare a unei curbe asupra unui mesaj.
- prezentarea unor exemple pentru fiecare metodă.
- compararea metodelor din punct de vedere al complexității și al siguranței.
- descrierea unei metode originale (bazată pe metodele descrise) și descrierea îmbunătășirilor făcute.

Pentru a comunica, Alice și Bob fixează, mai întâi, curba eliptică $E(F_p)$ și punctul $P \in E$. Acestea pot fi făcute publice. Fiecare dintre ei își va alege câte un întreg care va fi de fapt cheia secretă a fiecăruia. Să notăm cei doi întregi cu q pentru Alice și respectiv r pentru Bob. Cei doi vor face publice și valorile $q * P$ și $r * P$. Pentru ca Alice să-i trimită lui Bob mesajul m ea îi va aplica mai întâi curba E obținând astfel un punct $P_m \in E$. Ea va cripta punctul P_m astfel:

$$C_1 = k * P \quad C_2 = P_m + k(r * P)$$

unde k este un număr ales de Alice la întâmplare.

Pentru a decripta, Bob va efectua următoarea operație:

$$C_2 - r * C_1 = P_m + k(r * P) - r(k * P) = P_m$$

Algoritmul prezentat mai sus este cunoscut ca Elgamal EC.

31. Să se implementeze un algoritm pentru acest sistem folosind metoda lui Koblitz pentru aplicarea curbei asupra mesajului.

32. Să se implementeze un algoritm pentru acest sistem folosind corespondența între literele alfabetului și numere pentru aplicarea curbei asupra mesajului.

33. Să se scrie o lucrare autentificare și autorizare în criptografie. Lucrarea va conține:

- descrierea termenului de autentificare și celui de autorizare din punct de veder criptografic.
- descrierea metodelor existente de autentificare.
- avantaje și dezavantaje ale metodelor descrise mai sus.
- descrierea unei metode originale de autorizare și prezentarea îmbunătățirilor aduse.

Avem protocolul:

1. Alice dorește să-i trimită lui Bob cheia sa; ea începe cu două stringuri de biți, a și b, fiecare având o lungime de n biți.
2. Apoi criptează aceste două stringuri ca un string de n qubiți:
$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle$$
unde a_i și b_i sunt ai i-ia biți din a și respectiv b.
3. Împreună $a_i b_i$ ne dau un index pentru următoarele patru stări ale qubiților:
$$|\psi_{00}\rangle = |0\rangle$$
$$|\psi_{10}\rangle = |1\rangle$$
$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$
Bitul b_i decide în ce bază este criptat a_i (baze computaționale sau baza Hadamard).
4. Alice îi trimite lui Bob $|\psi\rangle$ printr-un canal cuantic.
5. Bob primește o stare $\varepsilon\rho = \varepsilon|\psi\rangle\langle\psi|$ unde ε reprezintă efectul zgomotului din canal și al schimbările cauzate de un atacator, Eve.
6. După ce Bob primește qubiții, toate cele trei părți, Alice , Bob și Eve au propriile lor stări.
7. Mai departe, Bob generează un string de biți b' cu aceeași lungime ca b, și apoi măsoară stringul primit de la Alice rezultând a'.
8. După acest pas Alice face publică baza b.
9. Bob comunică cu Alice printr-un canal public pentru a determina care $b'_i \neq b_i$
10. Alice și Bob descarcă qubiții în a și a' unde b și b' nu se potrivesc.
11. Din cei k biți rămași, Alice alege aleator $k/2$ biți și-i face publici.
12. Alice și Bob verifică dacă un biții care diferă sunt într-un număr mai mare decât prevedeau ei.
13. Dacă se întâmplă acest lucru, cei doi reiau protocolul de la început, altfel protocolul s-a încheiat cu succes.

Acest protocol este cunoscut sub numele de BB84.
34. Să se implementeze un algoritm pentru acest protocol.
35. Să se determine vulnerabilitățile acestui protocol și să se corecteze pe cât posibil. Să se implementeze noul algoritm corectat.
36. Să se scrie o lucrare despre criptografia cuantică. Lucrarea va conține:

- descrierea acestui tip de criptografie
- descrierea metodelor existente.
- avantaje și dezavantaje ale metodelor descrise mai sus.
- compararea acestor metode cu metodele obișnuite.

37. Să se aleagă o metodă de stenografie și să se codeze un text.
38. Să se aleagă o metodă de stenografie și să se codeze o informație în cadrul unei imagini.
40. Să se scrie o lucrare despre combinarea criptografiei cu biometria. Lucrarea va conține:

    - descrierea termenului de biometrie.
    - descrierea metodelor de autentificare biometrică.
    - compararea acestora cu metodele de autentificare obișnuite.
    - avantaje și dezavantaje aplicării biometriei în criptografie.
    - prezentarea unei idei originale pentru o autentificare biometrică.