Capitolul 27

Teste grilă

27.1 Exerciţii

1. Completaţi: Scopul cifrării este de a asigura ..... unei comunicaţii.

   (a) autenticitatea

   (b) confidentialitatea

   (c) integritatea

   (d) nerepudierea

2. Următorul text a fost obţinut utilizând sistemul de cifrare Cezar (au fost eliminate accentele, spaţiile si semnele de punctuaţie): MHPEUDVVHPRQULYDOPDLVFHVWSRXUOHWRXIIHU. Care este decriptarea sa?

   (a) Chacun semble des yeux approuver mon courroux.

   (b) Ma bouche mille fois lui jura le contraire.

   (c) J'embrasse mon rival mais c'est pour l'etouffer.

   (d) De grâce, apprenez-moi, Seigneur, mes attentats.

3. Cifraţi textul "Attaque à l'aube " cu ajutorul algoritmului de substituţie precizat mai jos.

A	B	C	D	E	F	G	H	I	J	K	L	M
J	G	F	K	P	R	M	T	S	V	Z	D	Q

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
I	Y	B	C	W	A	O	X	E	H	N	U	L

   Care este textul cifrat obţinut?

(a) JOOJCXPJDJXGP

(b) SHHSMYVSWSYPV

(c) JOOJCXPJBJXGP

(d) SHHSMYVSZSYPV

4. Cifrul Vigenère reprezintă o modalitate de cifrare îmbunătăţită a sistemelor de cifrare cu substituţie simplă. În ce constă acesta?

   (a) în aplicarea succesivă a mai multor substituţii alfabetice pe acelaşi text.

   (b) în aplicarea de substituţii alfabetice care nu cifrează niciodată o literă în ea însăşi.

   (c) în cifrarea literelor care apar cel mai frecvent (cum ar fi e) în mai multe simboluri diferite.

   (d) în alegerea mai multor alfabete de sustituţie independente şi schimbarea alfabetului folosit, la fiecare literă, în mod ciclic.

5. Reprezentarea în baza 2 a numărului 1729 este:

   (a) 10010110100

   (b) 11011000001

   (c) 11001100011

   (d) 6C1

6. Propunem următorul algoritm de cifrare: Alice şi Bob doresc să schimbe un mesaj m care reprezintă un număr întreg între 0 şi $N-1$. Pentru aceasta, ei partajează o cheie secretă comună k extrasă aleator între 0 şi $N-1$. Mesajul cifrat se obţine ca $c = m+k \mod N$. Ce părere aveţi despre securitatea sistemului?

   (a) Proastă: sistemul reprezintă o variantă a sistemului lui Cezar.

   (b) Bună, dacă adversarul nu cunoaşte algoritmul de cifrare.

   (c) Foarte bună, cu condiţia să nu utilizeze cheia k decât o singură dată.

   (d) Excelentă: sistemul reprezintă o variantă a algoritmului RSA.

7. Alice îi trimite lui Bob un mesaj cifrat c obţinut cu ajutorul algoritmului precedent. Cum determină Bob mesajul original m?

   (a) $m = c + k \mod N$

   (b) $m = c - k \mod N$

   (c) $m = c \times k \mod N$

   (d) $m = c^k \mod N$

8. Care dintre acronimele următoare desemnează un algoritm de cifrare de tip bloc?

   (a) AES
   (b) HMAC
   (c) SHA-1
   (d) NIST

9. Inversul lui 17 modulo 100:

   (a) este 83.
   (b) este 53.
   (c) este 1/17.
   (d) nu există.

10. Am în posesia mea un mesaj m pe care nu vreau încă să îl divulg, dar doresc să pot dovedi peste câţiva ani că îl cunoşteam deja în 2010 (conform amprentei de timp). Pentru aceasta, este suficient să public astăzi:

    (a) un text cifrat corespunzător lui m cu o cheie cunoscută numai de mine.
    (b) un text cifrat corespunzător lui m cu o cheie cunoscută de toată lumea.
    (c) imaginea lui m printr-o funcţie de dispersie (funcţie hash).
    (d) imaginea lui m printr-un MAC folosind o cheie aleatoare.

11. Funcţia de dispersie (hash) SHA-512 întoarce valori între 0 şi $2^{512} - 1$. Se calculează imagini prin această funcţie în mod aleator. Care este ordinul de mărime al numerelor pentru care trebuie calculate valorile prin aceasta funcţie pentru a găsi 2 valori care să aibă primii 20 de biţi egali?

    (a) 20
    (b) 1000
    (c) 1000000
    (d) 2^{512}

12. Construim un generator de numere pseudo-aleatoare care iniţializează cu x_0 cu o valoare între 0 şi 999 şi determină $x_{n+1} = 500x_n + 789 \bmod 1000$. În ce condiţii aţi utiliza acest generator?

    (a) Pentru a produce numere aleatoare între 0 şi 999, dacă nu prezintă interes nivelul de securitate.
    (b) Pentru generarea unei chei de tip *one-time pad*.
    (c) Pentru construcţia unei funcţii de dispersie.

(d) Niciodată.

13. Cum este obţinută cheia secretă necesară pentru criptarea comunicaţiei, la conectarea la un site web securizat?

(a) Se obţine din parola introdusă pentru conectare, printr-un algoritm de derivare a cheii precum PBKDF (Password Based Key Derivation Function).

(b) Provine din cheia publică a serverului, conţinută într-un certificat.

(c) Provine din cheia privată a serverului, divulgată clientului după stabilirea conexiunii.

(d) Se obţine în urma unui schimb de chei între client şi server, precum schimbul de chei Diffie-Hellman.

14. Care este dificultatea de a factoriza un număr prim pe 1024 de biţi astăzi?

(a) Este simplu!

(b) Numărul poate fi factorizat cu ajutorul a câteva mii de calculatoare actuale care să ruleze între 1 şi 2 ani.

(c) Nimeni nu poate face asta momentan, dar poate se va reuşi de către agenţii precum NSA.

(d) Acest lucru nu va fi posibil timp de mai multe milenii.

15. Algoritmul RSA (fără padding) este un algoritm de cifrare:

(a) simetric, tip bloc.

(b) simetric, tip fluid (debit).

(c) parţial homomorfic.

(d) bazat pe identitate.

16. Fie generatorul Geffe descris de trei registre de deplasare $\mathbf{LFSR}_i$ (ale căror polinoame de feedback sunt primitive de grad 19, 21 şi respectiv 24) iar ieşirea de formula: $y(t) = a_1(t) \cdot a_3(t) \oplus \bar{a}_1\ (t) \cdot a_2(t)$. Care este complexitatea $\mathbf{LC}$ şi perioada $\mathbf{P}$ a acestui generator?

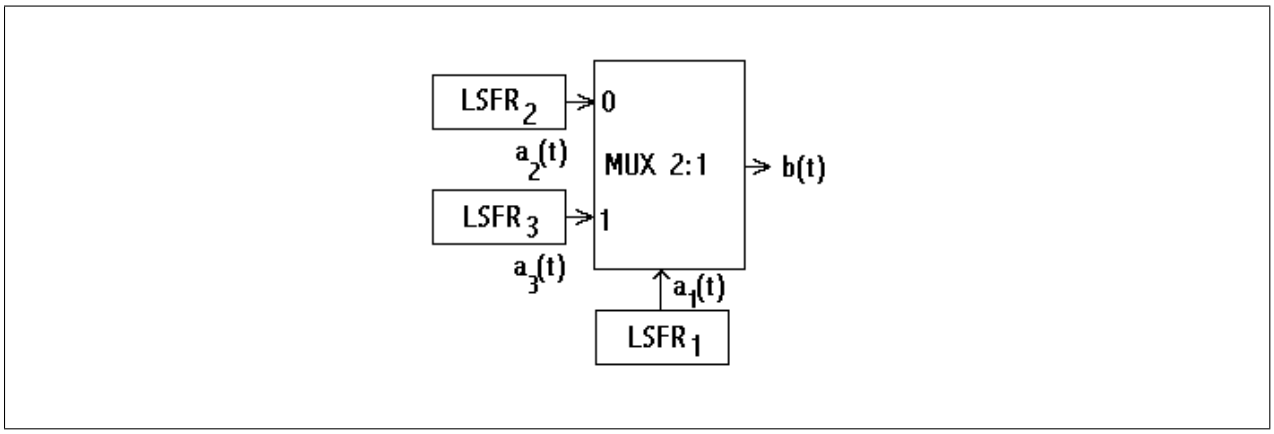

Figura 27.1: Generatorul Geffe.

(a) **LC**= 640, **P**= 2^{64}.

(b) **LC**=64 , **P**=$(2^{19}-1)(2^{21}-1)(2^{24}-1)$.

(c) **LC**=876 , **P**=$(2^{19}-1)(2^{21}-1)(2^{24}-1)$.

(d) Nici unul dintre răspunsuri nu este corect.

17. Fie secvenţa dată de reprezentarea binară (scrisă pe 8 biţi) a numărului i, $i = 0, ..., 255$:

$\underbrace{00000000}\ \underbrace{00000001}\ \underbrace{00000010}\underbrace{00000011}\underbrace{00000100}...\underbrace{11111111}$

Care este statistica testului frecvenţei aplicată acestei secvenţe binare? Este secvenţa aleatoare, relativ la testul frecvenţei, la riscul de ordinul 1 de 5%?

(a) $f_{tf} = 256$, şirul nu este aleatoriu.

(b) $f_{tf} = 1$, şirul este aleatoriu.

(c) $f_{tf} = 0$, şirul este aleatoriu.

(d) nici unul dintre răspunsuri nu este corect.

18. Care dintre următoarele afirmaţii sunt adevărate:

(a) Atac reuşit asupra a două preimagini ale unei funcţii hash implică reuşita atacului de generare de coliziuni.

(b) Atac reuşit de generare de coliziuni asupra unei funcţii hash implică reuşita atacului asupra a două preimagini a aceleiaşi funcţii hash.

19. Care dintre următoarele afirmaţii sunt adevărate:

(a) Un registru de deplasare de lungime n are perioada de $2^n - 1$.

(b) Un registru de deplasare de lungime n are perioada maximă de $2^n - 1$.

(c) Un registru de deplasare de lungime n, cu polinomul caracteristic primitiv, are perioada de $2^n - 1$.

20. Probabilitatea de coliziune a două mesaje de lungime n biţi procesate de aceeaşi funcţie hash ideală, ce are ieşirea pe m biţi, este:

(a) 2^{-m}.

(b) 2^{-n}.

(c) 2^{-mn}.

(d) 2^{m-n}.

(e) 2^{n-m}.

(f) Nici una din valorile de mai sus.