Criptografie

*Acest **curs** prezinta **Criptografie**.*
In acest PDF poti vizualiza cuprinsul si bibliografia (daca sunt disponibile) si aproximativ doua pagini din documentul original.
*Arhiva completa de pe site contine un fisier, intr-un numar total de **15 pagini**.*
Fisierele documentului original au urmatoarele extensii: pdf.

Extras

Cifruri monoalfabetice- Cu numai 25 de chei posibile, cifrul lui Cezar este considerat slab la atacurile criptanalitice.- Numarul de chei poate creste foarte mult daca se realizeaza o substitutie arbitrara. În acest caz exista 26! chei posibile.- Aceasta înseamna ca exista de 10 ori mai multe chei decât în cazul cifrului DES (cifrul DES având 256 chei).- Literele cifrului se pot obtine astfel: se alege prima litera A si apoi, în ordine ciclica fiecare a treia litera, adica D,G,...,Y.- Dupa litera Y sirul cifrului se continua cu B, deoarece, în ordine ciclica, a treia litera dupa Y în alfabetul primar este B s.a.m.d. Astfel cifrul obtinut prin operatia de selectare este dat de relatia: C = 3p mod 26.

Introducere in Criptografie 3

Cifruri polialfabetice- Cifrurile polialfabetice constau din utilizarea periodica a unor substitutii simple diferite.- Fie d alfabete de cifrare C1, C2 ,..., Cd si d functii fi care realizeaza substitutia de forma: ƒ fi : A ’ Ci , 1 <= i <= d- unde A este alfabetul mesajelor în clar.- Un mesaj clar M = m1m2 ... md md+1... m2d va fi cifrat prin repetarea secventelor de functii f1 ,..., fd la fiecare al d-lea caracter: ƒ E(M) = f1 (m1)... fd (md) f1 (md+1).- În acest caz numarul cheilor posibile se mareste de la 26! la (26!)n .

Introducere in Criptografie 4

Cifrul Vigenere- Functiile fi de substitutie se definesc astfel: fi (a) = (a+ ki)(mod n) unde n este lungimea alfabetului, ki este litera cheii k= k1 k2 ... kd, iar a este litera din mesajul clar.- Se considera cheia de opt litere “academie” care va fi utilizata repetitiv pentru cifrarea mesajului “substitutie polialfabetica”.

. . . . . .
. . . . . .
. . . . . .

Imagini din documentul complet:

Cifruri transpoziție

- Cifrurile transpoziție realizează o permutare a caracterelor din textul clar.
- Cheia de cifrare este perechea $k=(d, f)$, unde d reprezintă lungimea blocurilor succesive de caractere care vor fi cifrate conform permutării f:

$$f: Z_d \to Z_d,\ Z_d = \{1,2,\ldots,d\}$$

de forma

1	2	…	d
f(1)	f(2)	…	f(d)

unde $f(i) \neq f(j)$, pentru orice $i \neq j$.

- Mulțimea funcțiilor astfel definite este d!. În acest fel mesajul clar $M = m_1 m_2 \ldots m_d m_{d+1} \ldots m_{2d} \ldots$ este cifrat astfel:

$$C = E_k(M) = m_{f(1)} \ldots m_{f(d)}\ m_{f(d+1)} \ldots m_{d+f(d)} .$$

Cifruri transpoziție

- Descifrarea se obține prin permutarea inversă.
- Cifrarea prin transpoziție este o transformare a textului clar prin care se modifică poziția caracterelor în mesaj.
- O metodă des folosită pentru implementarea acestui tip de transformare este scrierea mesajului într-o anumită matrice după care textul cifrat se obține prin citirea caracterelor pe linie, pe coloană sau după un anumit traseu în matrice.
- Cele mai simple transpoziții se obțin prin împărțirea textului clar în două jumătăți care se scriu una sub alta, după care se citesc coloanele de la stânga la dreapta. De exemplu, cuvântul "calculator" se cifrează astfel:

Text clar: c a l c u
l a t o r

Text cifrat: CLAALTCOUR

Cifrul DES

- Cel mai utilizat algoritm de criptare simetric este algoritmul DES (Data Encryption Standard) adoptat în 1977 de către Biroul Național de Standarde, acum Institutul Național de Standarde și Tehnologie (NIST) din SUA.
- Sistemul DES este primul standard dedicat protecției criptografice a datelor de calculator.
- DES este un cifru bloc, cu lungimea de 64 biți prelucrați în conjuncție cu o cheie formată din 56 biți.
- Mai sunt folosiți 8 biți pentru detectarea erorilor de transmisie. Această cheie este păstrată de către toți membrii grupului care, astfel, pot cifra/descifra datele transmise de la unii la alții.
- Privit în ansamblu, algoritmul DES este o combinație a două tehnici elementare de criptare: confuzie și difuzie.