SISTEME SIMETRICE DE CRIPTARE MODERNE

DES (Data Encryption Standard)

I. Descrierea sistemului de criptare DES

Vizualizați în Cryptool cum funcționează sistemul de criptare DES (*DES Visualization*).

II. Criptare

Criptaţi mesajul ***HORST FEISTEL***.

i. Folosiţi cheia de criptare ***AB CD EF 01 23 45 67 89***.
ii. Utilizaţi mai întâi modul de criptare ECB, apoi în modul de criptare CBC.

III. Decriptare

i. Consideraţi aceeaşi cheie de mai sus.
ii. Decriptaţi mesajul:

C6 C4 EB DC 90 D3 42 F5 48 FD 7E C5 15 9A 87 4F 1A FF A2 13 A5 9B E7 F7 49 5E F4 44 39 DB 63 61

iii. În ce mod s-a realizat criptarea, ECB sau CBC?

IV. Proprietatea de difuzie

i. Alegeţi un text clar oarecare.
ii. Alegeţi o cheie oarecare (dar nu trivială).
iii. Criptaţi textul în mod ECB cu ajutorul cheii şi păstraţi textul criptat obţinut.
iv. Modificaţi un singur bit din cheia de criptare.
v. Criptaţi din nou textul, utilizând această nouă cheie.
vi. Ce observaţi?

V. Rezistenţa la erorile de transmisie – modurile de implementare ECB şi CBC

i. Alegeţi un text clar oarecare.

ii. Alegeţi o cheie oarecare (dar nu trivială).
iii. Criptaţi textul clar în modul ECB.
iv. În textul criptat obţinut modificaţi un singur bit
v. Decriptaţi textul astfel modificat.
vi. Repetaţi paşii iii-v pentru modul CBC (păstraţi constantă poziţia bitului pentru cele 2 moduri).

Care dintre cele 2 moduri este mai rezistent la erorile de transmisie?

VI. Chei slabe şi perechi de chei semi-slabe

i. Se consideră următoarele chei:

01 01 01 01 01 01 01 01

01 E0 01 E0 01 F1 01 F1

10 10 10 10 10 10 10 10

E0 01 E0 01 F1 01 F1 01

ii. Care dintre acestea este o cheie slabă ?
(i.e. $e_k(e_K(M))=M$, pentru orice mesaj M)

iii. Puteţi găsi o pereche de chei semi-slabe?
(i.e. $e_{k1}(e_{K2}(M))=M$, pentru orice mesaj M)

VII. Meet-In-The-Middle Attack

i. Se dă textul clar:

des

ii. Se ştie că acesta a fost supus unei duble criptări cu DES în mod ECB, folosind 2 chei de forma:

X0 00 00 00 00 00 00 00

unde X poate fi orice cifra hexazecimală.

iii. În urma acestei criptări s-a obţinut textul criptat:

±$^VyuQ¢

(B1 24 5E 56 79 75 51 A2)

iv. Folosind un atac de tip Meet-In-The-Middle determinaţi cele 2 chei.

AES (Advanced Encryption Standard)

I. Descrierea sistemului de criptare AES

Vizualizați în Cryptool cum funcționează sistemul de criptare AES (*AES Visualization*).

II. Criptare

i. Folosiţi cheia de criptare pe 128 de biţi:

AB CD EF 01 23 45 67 89 AB CD EF 01 23 45 67 89

ii. Criptaţi textul ***Advanced Encryption Standard***

III. Decriptare

Folosind aceeaşi cheie de criptare de la punctul II şi padding mode *1-0 padding*, decriptaţi mesajul:
68 8F C9 EB BF 35 0A 54 48 22 4D D7 DB E3 AA 9B CB 06 81 96 77 56 AA 76 7F A3 D5 75 DF 33 E7 BE

ⓘ Mai multe informaţii:

1. CrypTool Portal (Cryptool 2)
https://www.cryptool.org/en/
2. ECE646 - Lab#3 – Kryptos – Properties of secret-key ciphers
http://www.docstoc.com/docs/34482238/ECE646-Lab-3-Kryptos---Properties-of-secret-key
3. NIST – Data Encryption Standard (DES)
http://www.itl.nist.gov/fipspubs/fip46-2.htm
4. AES Proposal: Rijndael
http://www.daimi.au.dk/~ivan/rijndael.pdf
5. Block cipher modes of operation
http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation
6. NIST – Advanced Encryption Standard (AES)
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf