

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

Criptați mesajul **HORST FEISTEL**.

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

III. Decriptare

- i. Considerați aceeași cheie de mai sus.
- ii. Decriptați mesajul:

**68 41 43 0D 6C 80 81 A5 00 2F CD 0B 55 23 AA 87 25 03 F7 D9 22 FD 99 71
7F A1 72 E9 B8 B0 90 EC**

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

IV. Proprietatea de difuzie

- i. Alegeți un text clar oarecare.
- ii. Alegeți o cheie oarecare (dar nu trivială).
- iii. Criptați textul în mod ECB cu ajutorul cheii și păstrați textul criptat obținut.
- iv. Modificați un singur bit din cheia de criptare.
- v. Criptați din nou textul, utilizând această nouă cheie.
- vi. Ce observați?

V. Rezistența la erorile de transmisie – modurile de implementare ECB și CBC

- i. Alegeți un text clar oarecare.

- ii. Alegeți o cheie oarecare (dar nu trivială).
 - iii. Criptați textul clar în modul ECB.
 - iv. În textul criptat obținut modificați un singur bit
 - v. Decriptați textul astfel modificat.
 - vi. Repetați pașii iii-v pentru modul CBC (păstrați constantă poziția bitului pentru cele 2 moduri).
- Care dintre cele 2 moduri este mai rezistent la erorile de transmisie?

VI. Chei slabe și perechi de chei semi-slabe

- i. Se consideră următoarele chei:

01 E0 01 E0 01 F1 01 F1

10 10 10 10 10 10 10 10

FE FE FE FE FE FE FE FE

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. Puteți 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 știe 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 cifră hexazecimală.
- iii. În urma acestei criptări s-a obținut textul criptat:
äá-|pz|Ý
(E4 E1 96 5D 70 7A 7C DD)
- iv. Folosind un atac de tip Meet-In-The-Middle determinați 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. Folosiți cheia de criptare pe 128 de biți:

AB CD EF 12 34 56 78 90 AB CD EF 12 34 56 78 90

- ii. Criptați textul *Advanced Encryption Standard*

III. Decriptare

Folosind aceeași cheie de criptare de la punctul II și padding mode *I-0 padding*, decriptați mesajul:

***33 7B 1D A6 7B C6 0E 9C AF 32 0A A2 BA DF 12 BA 3A A7 A6 8A 23
B2 40 EC 2A 14 15 45 7E D1 3A A5***

① Mai multe informații:

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>