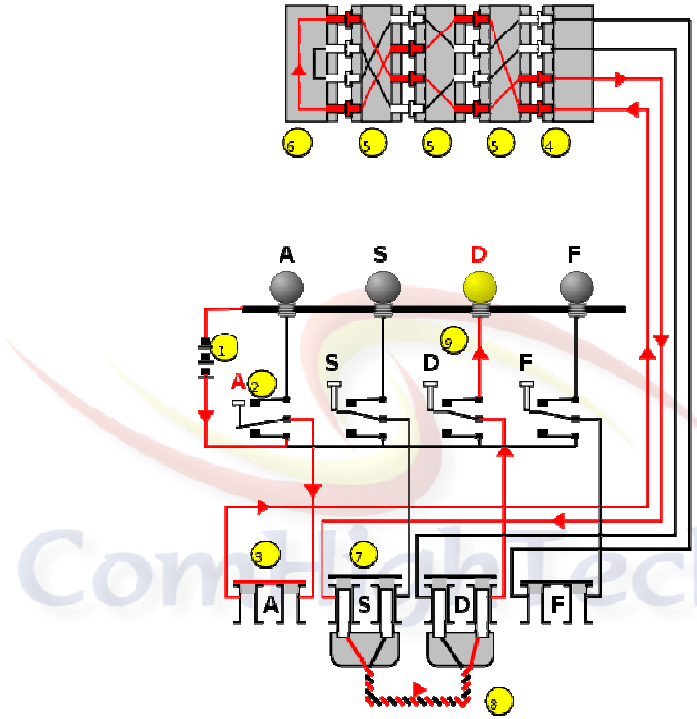
UNIUNEA EUROPEANĂ
GUVERNUL ROMÂNIEI MINISTERUL MUNCII, FAMILIEI ŞI PROTECŢIEI SOCIALE AMPOSDRU
Fondul Social European POSDRU 2007-2013
Instrumente Structurale 2007-2013
ORGANISMUL INTERMEDIAR REGIONAL PENTRU POS DRU REGIUNEA BUCUREŞTI ILFOV

Proiect cofinanțat din Fondul Social European prin
Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013.
"Investește în oameni!"

Cap. 2.1 Functii Criptografice Simetrice. Functii fara cheie: generatoare de numere pseudo-aleatoare si functii hash (MD5, SHA1, SHA2, SHA3). Functii cu cheie simetrica: coduri MAC (NMAC, HMAC) si criptari simetrice (DES, 3DES, AES).Securitatea Informatiei

Masina Enigma (studiu de caz clasic)



- Circuit din wiki

Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013.
"Investește în oameni!"

Setarea cheii la Enigma

- 3 rotoare (5 la varianta mai evoluata) care se pot aranja in orice ordine (sus)
- 26 de variante de a aseza fiecare rotor
- 26 de puncte in care putea sa cupleze fiecare rotor
- O tabela cu 26 litere cuplabile 2 cate 2 prin max. 13 stechere (partea frontala)
- Observatie: cablajul rotoarelor era standard produs din fabrica, dar in principiu se putea extinde cu un cablaj custom

UNIUNEA EUROPEANĂ
GUVERNUL ROMÂNIEI MINISTERUL MUNCII, FAMILIEI ŞI PROTECŢIEI SOCIALE AMPOSDRU
Fondul Social European POSDRU 2007-2013
Instrumente Structurale 2007-2013
ORGANISMUL INTERMEDIAR REGIONAL PENTRU POS DRU REGIUNEA BUCUREŞTI ILFOV

Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013. "Investește în oameni!"

Cat de puternica este Enigma

- Una dintre masurile de baza cu privire la securitatea unui criptosistem este dimensiunea spatiului din care provibe cheia
- Cate variante de a cupla *p* stechere sunt? Care este dimensiunea spatiului cheii? Dar daca cablajul fiecarui rotor putea fi setat? Calculati spatiul cheilor la Enigma si comparati cu DES (56), 3DES, AES (128).

Cat de slaba este Enigma

Intrebare interesanta de la cursurile crypt@b-it 2007 Bonn, Germania

(ii) "Cribs" are stereotypical parts of a message. E. g.
WETTERBERICHT (weather report)
OBERKOMMANDO (supreme command)
KEINEBESONDERENVORKOMMNISSE (no notable events)
If the ciphertext started with GBDQQBHNWZTA, the message can start with only one of the above cribs. Which one?

Clasificarea functiilor criptografice

- Exista trei mari categorii de functii criptografice:
  - **Functii fara cheie** - nu utilizeaza cheie (unii autori le considera functii simetrice in baza principiului: nici o cheie inseamna aceeasi cheie de ambele parti). Exemplu de functii fara cheie: functii hash, generatoare PRNG.
  - **Functii simetrice** (cu cheie secreta) – utilizeaza aceeasi cheie de ambele parti. Exemple de functii simetrice: criptari simetrice (regula de decriptare se poate deduce usor cunoscand regula de criptare si reciproc), coduri de autentificarea a mesajelor (MAC).
  - **Functii asimetrice** (cu cheie publica) – utilizeaza chei diferite de partea celor doua entitati. Exemplu de functii asimetrice: criptari cu cheie publica (cheia privata nu poate fi calculata pe baza cheii publice – nu este tot timpul adevarat si reciproc), semnaturi digitale.

Functii one-way si trapdoor one-way (cu trapa)

- **Definitie** (intuitiva): O functie $f:X \rightarrow Y$ se numeste one-way daca f(x) este usor de calculat pentru orice $x \in X$ si pentru orice $y \in Im(f)$ este nefezabila gasirea unui $x \in X$ astfel incat $f(x)=y$
- **Definitie** (intuitiva): O functie one-way se numeste trapdoor one-way daca exista o informatie, numita trapdoor (trapa), in baza careia functia poate fi inversata
- **Observatie** (intuitiva): Orice functie trapdoor one-way poate fi baza unui sistem criptografic daca valoare trapei este cheia de decriptare si aceasta este greu de calculat pentru un adversar respectiv usor de calculat pentru cel care o genereaza

Functii fara cheie

- **Functii hash** se noteaza $H(x)$ - functie hash aplicata mesajului x. O functie hash este o functie one-way (ireversibila) care primeste ca intrare mesaje de dimensiune variabila si returneaza un mesaj de lungime fixa din care mesajul initial nu poate fi recuperat, aceste primitive nu folosesc nici un fel de cheie. Cea mai utilizata familie de functii hash este SHA (Secure Hash Algorithm) [FIPS 180-2, 2002] pentru care dimensiunea iesirii este 224, 256, 384, 512 biti indiferent de dimensiunea datelor de intrare.
- In general fata de o functie hash se impun cerintele:

a) Rezistenta primara a imaginii (sau *target collision resistance*): *avand* $H(x)$ *gaseste* x

b) Rezistenta secundara a imaginii: *avand* $x, H(x)$ *gaseste* x' *astfel incat* $H(x)=H(x')$

c) Rezistenta la coliziune: *gaseste* x, x' *astfel incat* $H(x)=H(x')$

Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013. "Investește în oameni!"

Functii hash (ce se foloseste in pratica azi)

- MD5 si SHA1 inca frecvente in practica, dar trebuie evitate pentru ca au vulnerabilitati (nu mai ofera rezistenta la coliziune)
- SHA2: SHA 256, SHA384, SHA 512 standardul curent, nu se cunosc vulnerabilitati
- SHA3: noul standard, competitia lansata in 2008, finalizata in 2010, si rezultatul standardizat in 2012

Coduri de autentificare a mesajelor MAC (Message Authentication Codes)

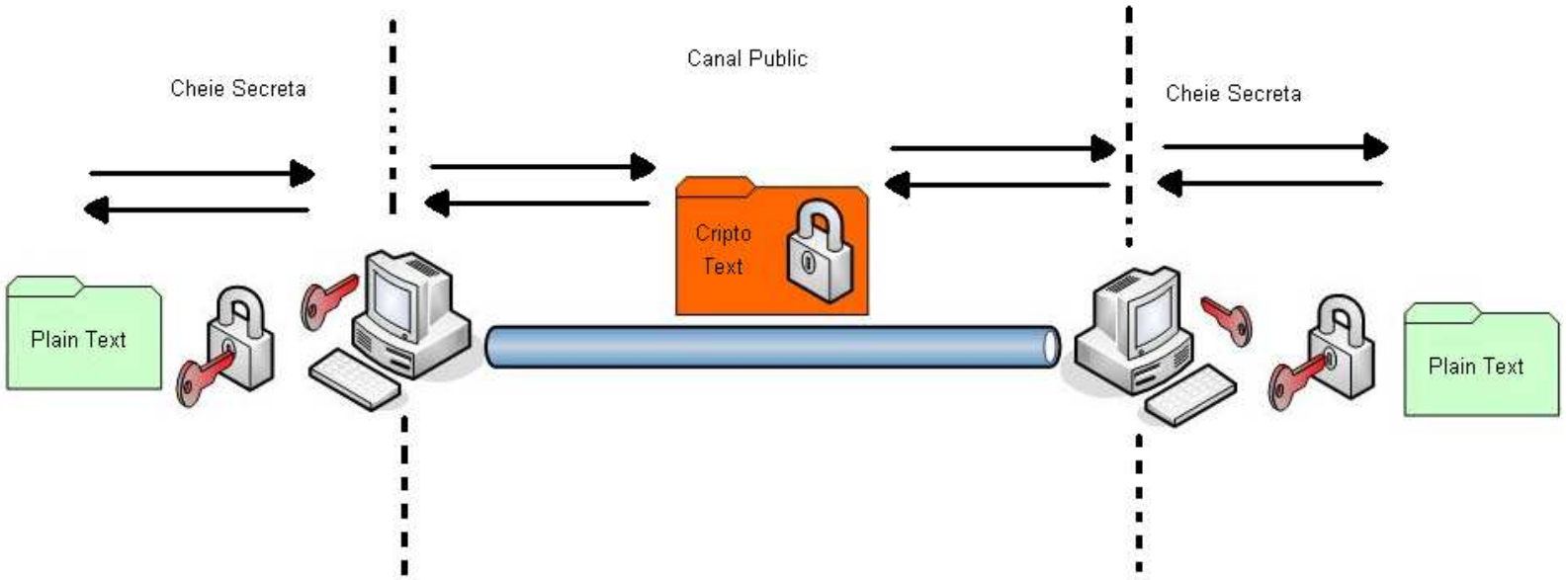
- **Coduri de autentificare a mesajelor** se noteaza $MAC_k(m)$ - cod de autentificare a mesajului m calculat cu cheia k).
- Se construiesc peste o functie hash (in general MD5 sau SHA1, MD5 cu toate ca ambele au un nivel de securitate destul de scazut)
- Se folosesc pentru a testa autenticitatea unei informatii – implica si o garantie asupra integritatii
- In practica se foloseste HMAC si NMAC propuse de Mihir Bellare, Ran Canetti, Hugo Krawczyk in lucrarea http://www-cse.ucsd.edu/users/mihir/papers/kmd5.pdf

Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013.
"Investește în oameni!"

Functii MAC (ce se foloseste in pratica azi)

- Constructille HMAC si NMAC propuse de Mihir Bellare, Ran Canetti, Hugo Krawczyk in lucrarea http://www-cse.ucsd.edu/users/mihir/papers/kmd5.pdf
- HMAC este prezenta in marea parte a limbajelor Java, .NET

Criptari simetrice



Criptari simetrice

- Sisteme criptografice care utilizeaza aceeasi cheie sau chei usor de calculat una pe baza celelilalte pentru criptare si decriptare (cheia este referita ca cheie secreta)
- Doua principii constructive:

1) **substituţia** – inseamna inlocuirea unor simboluri sau grupuri de simboluri prin alte simboluri sau grupuri de simboluri - creează **confuzie**

2) **transpoziţia** – inseamna amestecarea (permutarea) simbolurilor din cadrul unui bloc creează **difuziune**

- Doua clase de criptari simetrice:

1) **coduri bloc** - algoritmi de criptare care impart mesajul ce trebuie criptat in blocuri de dimensiune fixa *l* si cripteaza un bloc la un momemt dat

2) **coduri stream** -algoritmi de criptare pentru care cripteaza „caracter cu caracter" (practic lungimea blocului este 1, si transformarea de criptare se poate modifica pentru fiecare caracter)

Exemplu

- Exemplu: Codul Vernam (sau one-time pad) este un cod stream care presupune utilizarea unei chei aleatoare k de aceeasi dimensiune cu a mesajului m, criptotextul c este $c_i = m_i \, XOR \, k_i$ (se face XOR bit cu bit intre mesaj si cheie) (cheia nu poate fi reutilizata pentru transmiterea altui mesaj)
- Observatie: Se poate demonstra ca un sistem criptografic perfect, care sa nu poata fi spart, necesita o cheie aleatoare de aceeasi dimensiune cu a mesajului

Reteaua Feistel

- **Codul Feistel** este primul criptosistem simetric modern, marea parte a criptosistemelor simetrice contemporane urmeaza principiile codului Feistel (retea Feistel)
- Reteaua Feistel aplica urmatoarele transformari asupra plaintext-ului: permutari (P-boxes) pentru a crea difuzie, substitutii, pentru a crea confuzie (S-boxes) si operatii pe biti (XOR) in http://en.wikipedia.org/wiki/Feistel (in general este necesar un minim de 16 runde pentru securitate adecvata).
- Principii generale in reteaua Feistel: cu cat dimensiunea blocului, a cheii si numarul de runde creste, creste si securitatea respectiv scade viteza de criptare/decriptare, iar daca scad, scade si securitatea respectiv creste viteza de criptare/decriptare
- Marele avantaj este ca criptarea si decriptarea se fac parcurgand aceeasi retea in sens invers

DES (primul standard in criptografia simetrica)

- DES (Data Encryption Standard) este primul standard simetric, valabil pana in 2001 (in 1999 recomandat sub forma 3DES)
- DES este un cod simetric pe retea Feistel
- DES transforma plain-text de 64 de biti in criptotext de 64 de biti, cheia DES are doar 56 de biti. Poate fi usor spart in prezent si este scos din uz. Continua sa existe sub varianta 3DES care consta in aplicarea tranformarii DES de 3 ori si este pe 128 de biti. Descrierea criptosistemului http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf , http://en.wikipedia.org/wiki/Data_Encryption_Standard

AES (standardul curent in criptografia simetrica)

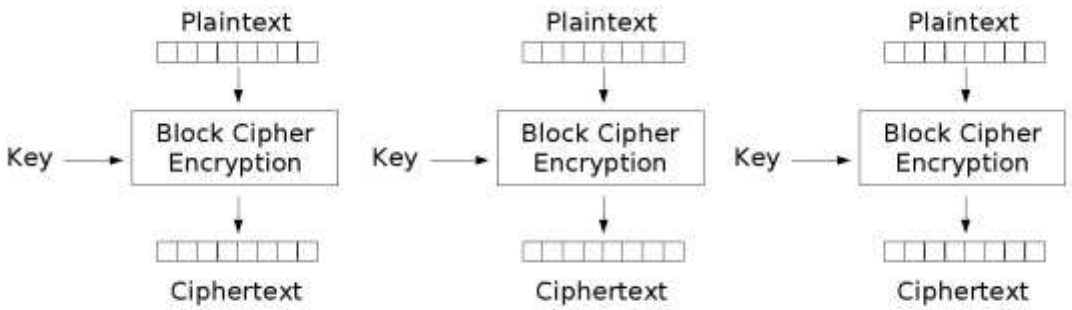
- La nivelul anilor 2001 DES nu mai ofera securitatea necesara, pentru care, pe baza de concurs se alege un nou standard AES (Advanced Encryption Standard)
- Din cei 5 finalisti: Rijndael, Serpent, Twofish, RC6 si MARS este ales candidatul Rijndael
- Rijndael este un cod bloc disponibil in 3 variante: 128, 192, 256 de biti. Descrierea criptosistemului http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf, http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
- Necesita doar 10-14 runde in functie de dimensiunea cheii, este sigur si rapid
- Un singur dezavantaj: are un design extrem de exotic comparativ cu toate celelalte criptosisteme simetrice, transformarea Rijndael este echivalenta cu o ecuatie algebrica destul de simpla (comprativ cu alte coduri) fata de care exista suspiciunea ca ar putea duce in viitor la o serie de atacuri http://www.macfergus.com/pub/rdalgeq.pdf

Functii de criptare simetrica

- Standardul curent AES disponibil cu chei pe 128, 192, 256 biti
- Nu sunt motive serioase pentru a folosi altceva
- Doar daca se doreste un design mai conservator, se poate recurge la contracandidatii lui AES
- 3DES este forma in care DES supravietuieste cu chei de 56, 112 (mai uzual) sau 168 biti – nu sunt motive serioase pentru a fi utilizat si se recomanda evitarea lui (cel putin din ratiuni de performanta/siguranta, de ex. varianta de 168 biti are o securitate echivalenta de NIST la nivel de 80 biti)

Moduri de functionare ale codurilor bloc

- Varianta ECB (Electronic Code Book) nesigura dar inca folosita de programatori (poza wiki)



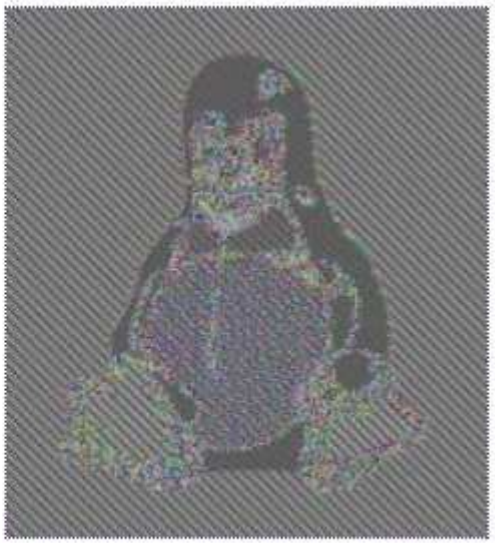
Electronic Codebook (ECB) mode encryption

- Variantele CBC (Cipher Block Chaining) si CM (Counter Mode) sunt sigure

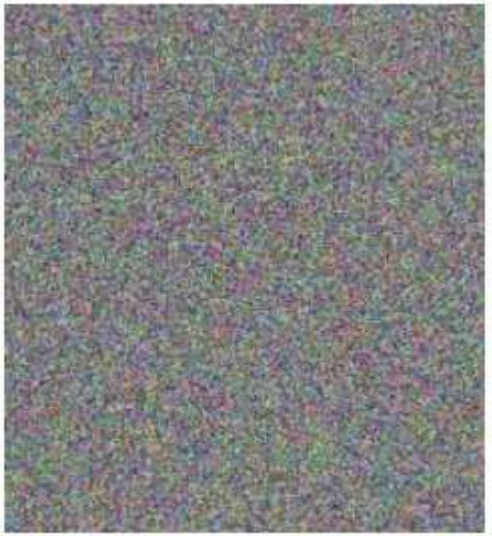
Lipsa de securitate in ECB

- Exemplu din http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Original

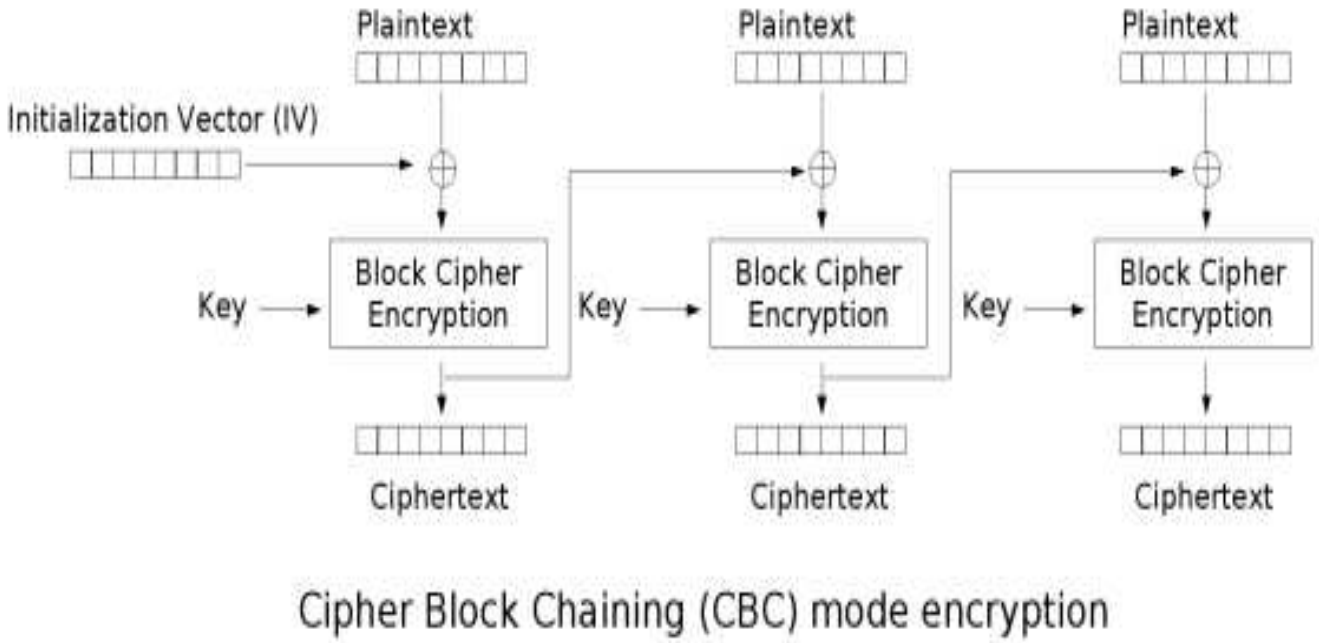


Encrypted using ECB mode



Other modes than ECB results in pseudo-randomness

Modul CBC

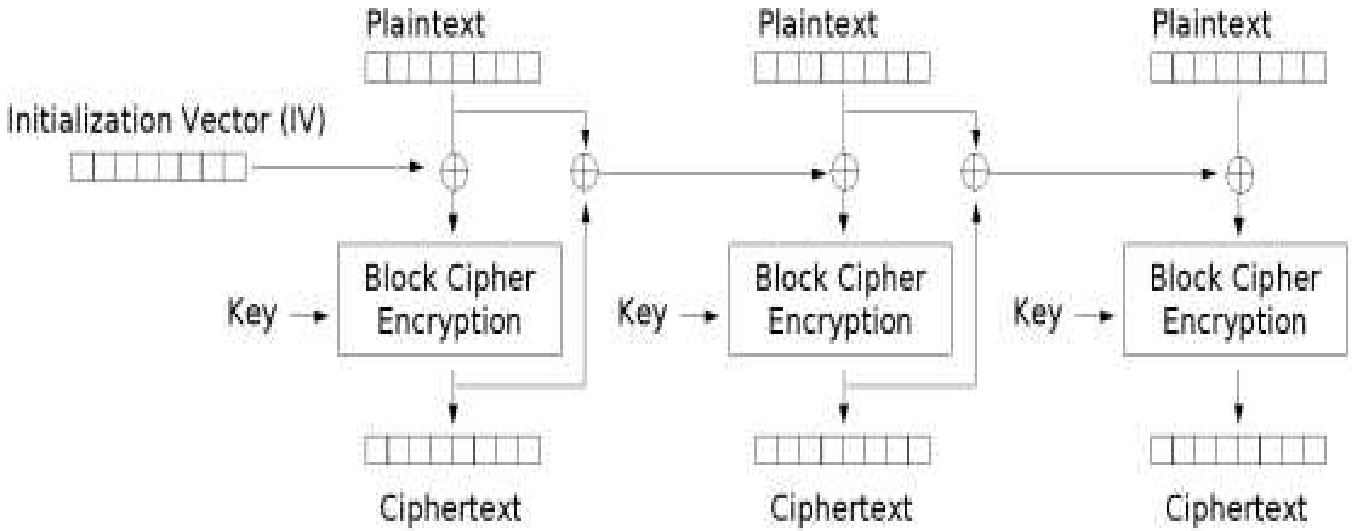


Cipher Block Chaining (CBC) mode encryption

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013.
"Investește în oameni!"

Modul PCBC

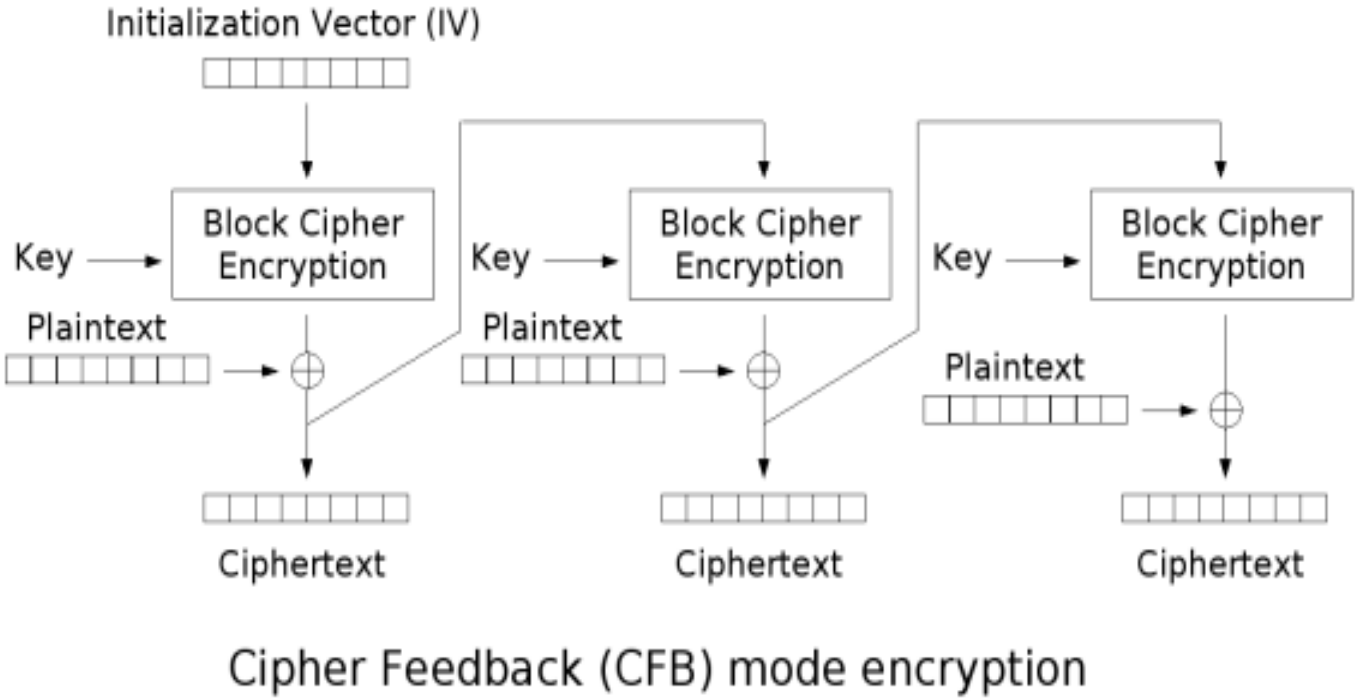


Propagating Cipher Block Chaining (PCBC) mode encryption

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013.
"Investește în oameni!"

Modul CFB

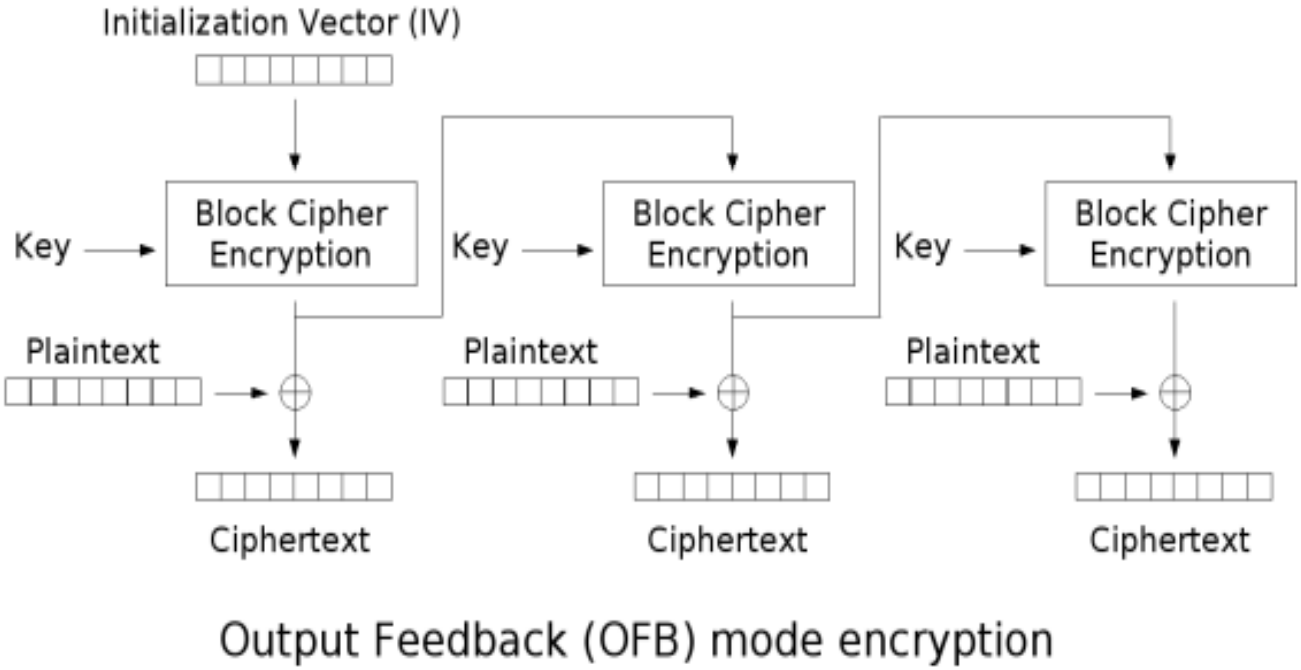


Cipher Feedback (CFB) mode encryption

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013.
"Investește în oameni!"

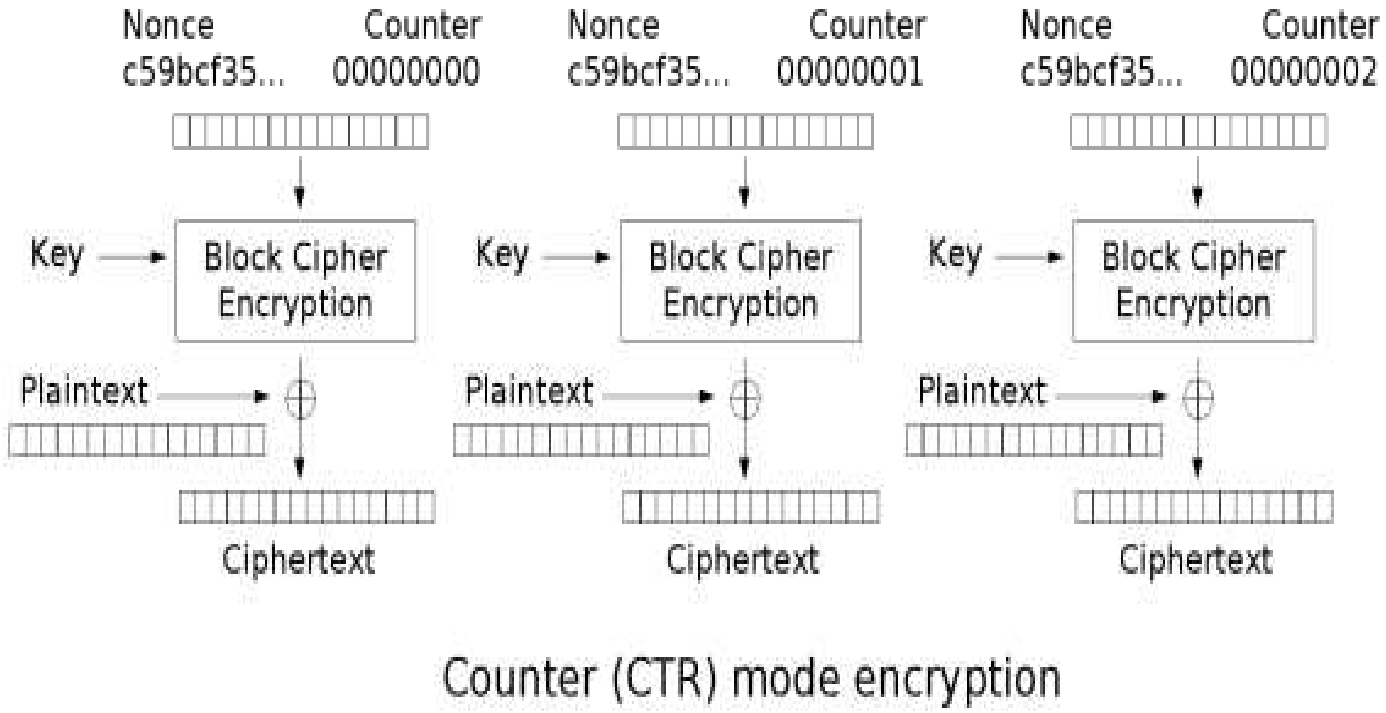
Modul OFB



Output Feedback (OFB) mode encryption

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Modul Counter



Counter (CTR) mode encryption

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Tipuri de atac asupra functiilor criptografice

- Scopul unui atac asupra unei functii criptografice este de a recupera plain-textul din cripto-text sau de a recupera cheia secreta:

1) **Criptotext cunoscut** (ciphertext-only) - adversarul cunoaste doar criptotextul.
2) **Plaintext cunoscut** (known plaintext)- adversarul cunoaste mai multe perechi (plaintext, ciphertext).
3) **Plaintext ales** (chosen plaintext) - adversarul alege plaintext-ul si primeste valoare criptotextului.
4) **Plaintext ales adaptiv** (adaptive chosen plaintext) - la fel ca la atacul plaintext ales doar ca alegerea se face in functie de raspunsurile anterioare.
5) **Criptotext ales** (chosen ciphertext) – adversarul alege criptotextul si primeste plaintextul.
6) **Criptotext ales adaptiv** (adaptive chosen ciphertext) – la fel ca la atacuri criptotext ales cu observatia ca fiecare alegere se face in functie de raspunsurile anterioare.