METODE CRIPTOGRAFICE DE PROTECȚIE A INFORMAȚIEI

Tema: Cifruri bloc moderne

MODURI DE IMPLEMENTARE A CIFRURILOR BLOC

În această secțiune sunt examinate două moduri de implementare a cifrurilor bloc cu cheie simetrică: ECB și CBC. Un mod de operare a cifrului bloc este un algoritm ce utilizează cifrul bloc pentru a cripta texte clare de dimensiuni mari, astfel încât să se asigure un nivel avansat de confidențialitate a datelor.

Amintim că cifrul bloc criptează și decriptează în mod securizat doar un singur bloc de text clar. Modul de operare descrie cum se va aplica repetat algoritmul de criptare/decriptare pentru a securiza criptarea / decriptarea textelor de lungime mai mare ca a unui bloc.

MODURI DE IMPLEMENTARE A CIFRURILOR BLOC

Nu este recomandat, pe cât este posibil, să se folosească aceeași cheie secretă pentru criptarea porțiunilor ce coincid ale textului clar. Utilizarea unui algoritm deterministic pentru un număr de texte clare identice, rezultă într-un număr de blocuri criptate identice. Un adversar poate să deducă informație suplimentară dacă cunoaște distribuția părților identice ale mesajului, chiar dacă nu este capabil să spargă cifrul și să afle mesajul inițial. Totuși, există căi ce permit ascunderea rezultatului aplicării cifrului bloc. Ideea constă în a amesteca blocurile de text clar cunoscut cu blocurile de text criptat care au fost generate anterior și utilizarea rezultatului la intrarea funcției de criptare, în vederea prelucrării următoarelor blocuri. În rezultat, se evită crearea de secvențe de text criptat identice din porțiuni identice de text clar, iar aceasta blochează stabilirea informației despre structura blocului. Aceste procedee sunt numite moduri de operare ale cifrurilor bloc.

MODURI DE IMPLEMENTARE A CIFRURILOR BLOC

De regulă, modurile de operare utilizează un șir binar, numit valoare de inițializare IV, unic pentru fiecare operație de criptare. Valoarea IV nu trebuie să se repete, iar în unele variante de algoritmi se alege aleator. Valoarea de inițializare IV este utilizată pentru a garanta generarea unor texte criptate distincte, chiar și atunci când este criptat de mai multe ori același text clar, în mod independent, cu aceeași cheie.

MODURI DE IMPLEMENTARE A CIFRURILOR BLOC

Textul clar este divizat pe blocuri (șiruri de biți de o anumită lungime), iar condițiile impuse asupra lungimii blocului variază în dependență de modul de operare utilizat. Unele moduri de operare a cifrurilor bloc (cum ar fi, ECB și CBC) folosesc blocuri complete (lungimea textului clar este un multiplu al lungimii blocului pentru sistemul de criptare utilizat) și necesită, eventual, ca ultimul bloc de date să fie completat (prin procedura de padding) până la un bloc complet. Există mai multe scheme de padding, cea mai simplă fiind cea în care șirul de biți ce reprezintă textul clar este completat cu biți de 0, până atunci când lungimea șirului devine un multiplu al lungimii blocului. O altă variantă de padding completează șirul inițial cu un bit de 1, după care urmează biți de 0.

MODURI DE IMPLEMENTARE A CIFRURILOR BLOC

Implementarea modului de operare a cifrului bloc prevede etapele de criptare și de decriptare.

Modul de operare	Textul criptat
ECB	$Y_i := E_K\left(BlocTextClar_i\right),\ TC := Y_i$
CBC	$BlocTextCriptat_0 := IV,\ Y_i := BlocTextClar_i \oplus BlocTextCriptat_{i-1},\ TC := E_K\left(Y_i\right)$
CFB	$BlocTextCriptat_0 := IV,\ Y_i := BlocTextCriptat_{i-1},\ TC := TextClar_i \oplus E_K\left(Y_i\right)$
OFB	$Y_i := E_K\left(I_{i-1}\right),\ Y_0 := IV,\ TC := TextClar_i \oplus Y_i$
CTR	$Y_i := E_K\left(IV + g\left(i\right)\right),\ IV := token(\ ),\ TC := TextClar_i \oplus Y_i$

Tabelul 1.3.1. Informație cu privire la modurile de operare

În continuare, pentru modurile ECB și CBC vom considera că textul clar constă din l blocuri de câte n biți, $x = x_1 \ldots x_l$, iar pentru CFB și OFB – din blocuri de s biți, unde $s \le n$ este fixat.

MODURI DE IMPLEMENTARE A CIFRURILOR BLOC

Este cel mai simplu mod de criptare, care, pentru o cheie dată, asociază fiecărui bloc de text clar un bloc de text criptat fixat.

Modul de operare ECB
Algoritmul de criptare ECB
Date de intrare: K - cheia pe m biți $x_1,\ldots,x_l$ - blocuri de text clar pe n biți fiecare Date de ieșire: $c_1,\ldots,c_l$ - blocuri de text criptat pe n biți fiecare
Pașii algoritmului: *Pentru* $j := \overline{1,l}$ *execută* { $c_j := E_k(x_j)$ }

MODURI DE IMPLEMENTARE A CIFRURILOR BLOC

Modul de operare ECB

Algoritmul de decriptare ECB

Date de intrare:

K - cheia pe m biți

$c_1,...,c_l$ - blocuri de text criptat pe n biți fiecare

Date de ieșire:

$x_1,...,x_l$ - blocuri de text clar pe n biți fiecare

Pașii algoritmului:

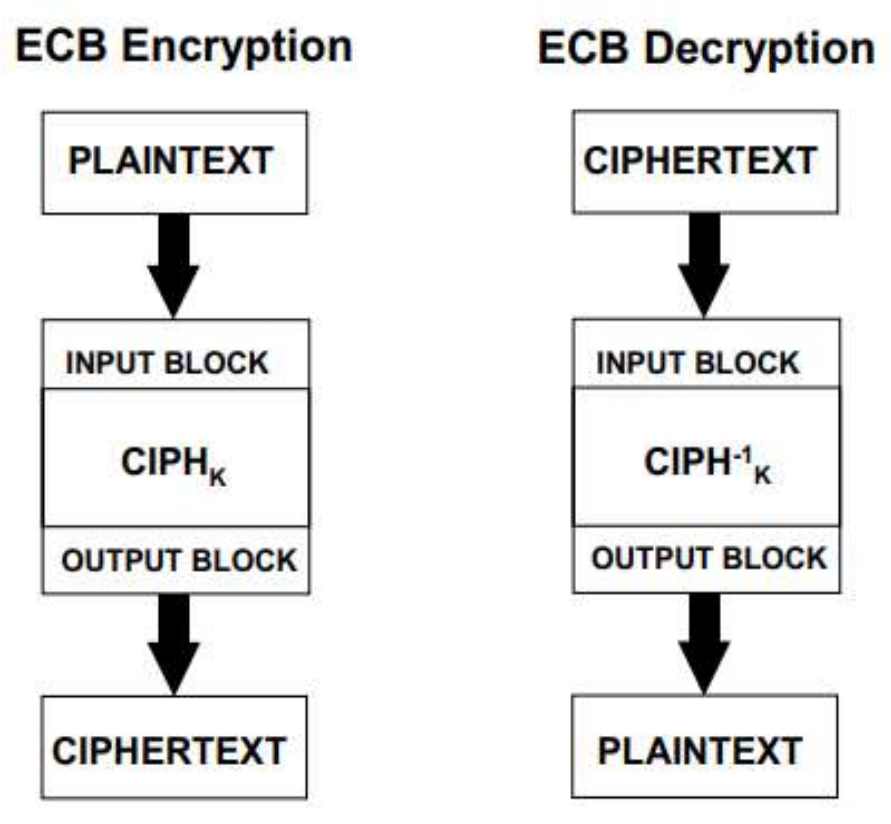
Pentru $j := \overline{1,l}$ *execută* { $x_j := D_k(c_j)$ }

MODURI DE IMPLEMENTARE A CIFRURILOR BLOC

Textul clar este divizat pe blocuri și fiecare bloc este criptat separat. Secvența de blocuri cifrate obținută formează textul criptat. Analog, fiecare bloc de text criptat este decriptat separat, iar secvența rezultată este textul clar. Astfel, este posibilă criptarea și decriptarea paralelă a mai multor blocuri.

Dezavantajul modului ECB este că blocurile de text clar identice sunt criptate (cu aceeași cheie) în blocuri identice de text criptat. Reordonarea blocurilor de text criptat rezultă în reordonarea corespunzătoare a blocurilor de text clar. Astfel, algoritmul ECB nu maschează suficient de bine șablonul datelor, prin urmare, nu promovează confidențialitate serioasă a mesajelor de lungime mai mare ca a unui bloc și nu este recomandat pentru utilizare în cadrul protocoalelor criptografice.

MODURI DE IMPLEMENTARE A CIFRURILOR BLOC



MODURI DE IMPLEMENTARE A CIFRURILOR BLOC

Acest mod de implementare a cifrurilor bloc a fost propus în anul 1976 în lucrarea [17] și este cel mai frecvent utilizat. Fiecare bloc de text clar, înainte de a fi criptat, este combinat printr-un XOR cu blocul precedent de text criptat. Astfel, fiecare bloc de text criptat depinde de toate blocurile de text criptat procesate până la moment. Pentru a face unic fiecare mesaj criptat, se va utiliza o valoare de inițializare IV pe n biți la criptarea primului bloc al mesajului. Valoarea de inițializare nu e necesar să fie secretă, dar trebuie să fie distinctă pentru fiecare mesaj (uneori se alege aleator).

Modul de operare CBC

Algoritmul de criptare CBC

Date de intrare:

K - cheia pe m biți

$x_1,...,x_l$ - blocuri de text clar pe n biți fiecare

IV - valoarea de inițializare pe n biți

Date de ieșire:

$c_1,...,c_l$ - blocuri de text criptat pe n biți fiecare

Pașii algoritmului:

$c_0 := IV$

Pentru $j := \overline{1,l}$ *execută* { $c_j := E_k\left(x_j \oplus c_{j-1}\right)$ }

MODURI DE IMPLEMENTARE A CIFRURILOR BLOC

Algoritmul de decriptare CBC

Date de intrare:

K - cheia pe m biți

$c_1,\ldots,c_l$ - blocuri de text criptat pe n biți fiecare

IV - valoarea de inițializare pe n biți

Date de ieșire:

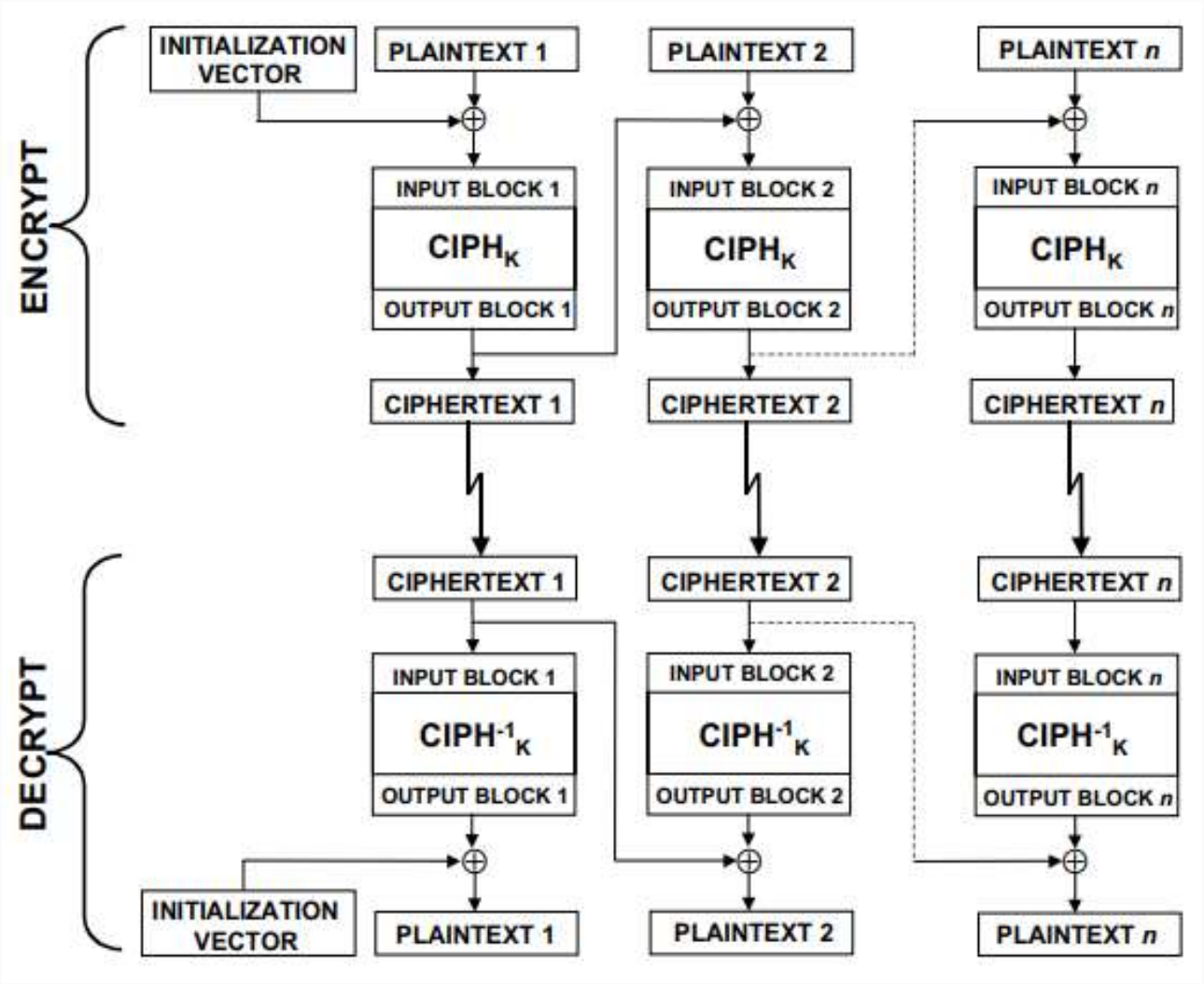
$x_1,\ldots,x_l$ - blocuri de text clar pe n biți fiecare

Pașii algoritmului:

$c_0 := IV$

Pentru $j := \overline{1,l}$ *execută* { $x_j := D_k\left(c_j\right) \oplus c_{j-1}$ }

MODURI DE IMPLEMENTARE A CIFRURILOR BLOC



Criptarea unor blocuri de text clar identice (cu aceeași cheie K și aceeași valoare inițială IV) generează blocuri identice de text criptat. Modificarea valorii IV sau a cheii conduce la texte criptate diferite.

Dezavantajele principale ale modului CBC sunt următoarele: criptarea se realizează secvențial (adică procedura nu poate fi realizată prin calcul paralel), iar lungimea mesajului trebuie să fie extinsă (prin procedura de padding) până la un multiplu al lungimii blocului de criptare. De menţionat că modificarea unui singur bit în textul clar sau în valoarea inițială IV afectează următoarele blocuri de text criptat.

Decriptarea cu o valoare inițială IV inexactă (și cheia K corectă) va genera un text clar cu primul bloc denaturat, celelalte blocuri fiind corecte. Aceasta se explică prin aceea că fiecare bloc de text decriptat este combinat printr-un XOR cu textul criptat al blocului precedent (și nu cu textul clar!). În consecință, procedura de decriptare CBC se poate efectua mai rapid (comparativ cu operația de criptare), printr-un proces de calcul paralel. De menționat că modificarea unui bit în blocul de text criptat conduce la denaturarea completă a blocului corespunzător de text clar și inversează bitul corespunzător în următorul bloc de text clar, iar restul blocurilor rămân intacte (adică modul CBC este auto-sincronizabil).

BIBLIOGRAFIE RECOMANDATĂ

1. A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
2. L. Knudsen, M. Robshaw, The block cipher companion, Springer, 2011.
3. J. Pieprzyk, T. Hardjono, J. Seberry, Fundamentals of Computer Security, Springer, 2003.
4. D. Stinson, M. Paterson, Cryptography: Theory and Practice, 4th ed., Boca Raton, FL: CRC Press, 2019.
5. D. Salomon, Data privacy and security, Springer, 2003.
6. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 20th Anversary Edition ed., Wiley, 2015.
7. FIPS PUB 46-3, "Data Encryption Standard (DES)," 1999 reaffirmed.
   https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf

BIBLIOGRAFIE RECOMANDATĂ

8. NIST Special Publication 800-67. Revision 1, "Recommendation for the Triple Data Encryption Algorithm (TDEA) block cipher," NIST - National Institute of Standards and Technology, 2012. https://csrc.nist.gov/publications/detail/sp/800-67/rev-2/final
9. J. Kilian, P. Rogaway, "How to protect against exhaustive key search," in *Proceedings of the CRYPTO'96, LNCS 1109*, 1996.
10. X. Lai, J. Massey, "A Proposal for a New Block Encryption Standard," in *EUROCRYPT 1990*, 1990.
11. Federal Information Processing Standards Publication 197, "Advanced Encryption Standard (AES)," National Institute of Standards and Technology, November, 2001. https://csrc.nist.gov/publications/detail/fips/197/final
12. J. Daemen, V. Rijmen, The design of Rijndael, AES- The Advanced Encryption Standard, Springer-Verlag, 2002.

BIBLIOGRAFIE RECOMANDATĂ

13. R. Anderson, E. Biham, L. Knudsen, "Serpent: A Proposal for the Advanced Encryption Standard," 1998.
14. B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, "Twofish: A 128-Bit Block Cipher," 1998.
15. NIST Special Publication 800-38A, "Recommendation for Block Cipher Modes of Operation: Methods and Techniques," National Institute of Standards and Technology, 2001.
https://csrc.nist.gov/publications/detail/sp/800-38a/final