Block ciphers

-Models and cryptographic techniques-

Emil SIMION
e-mail: esimion@fmi.unibuc.ro

Agenda

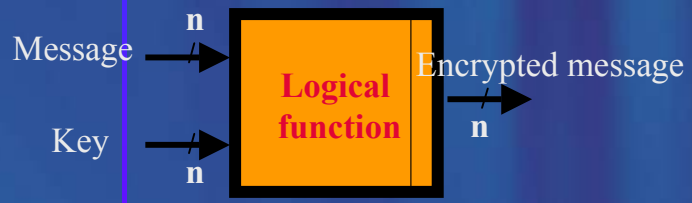
- Block cipher definition;
- Design criteria for block ciphers;
- Mode of operation of block ciphers;
- Evaluation, testing and cracking block ciphers;
- Linear cryptanalysis;
- Differential cryptanalysis, truncated differentials, impossible differentials;
- Example: boomerang attack;
- Example: AES (Advanced Encryption Standard);
- References;
- Questions and Answers.

Block cipher definiton

- Cryptographic primitive which ensures confidentiality of information;
- Characteristics of a block cipher are: block length and key length;
- Difference between block ciphers and stream ciphers is that the last one have a internal state and a transition function;
- Block ciphers are ideal for off-line encryption (storage protection) while stream ciphers are used for encrypting communication;
- There are methods for transformation a block cipher in a stream cipher and viceversa.

Block ciphers versus Stream ciphers

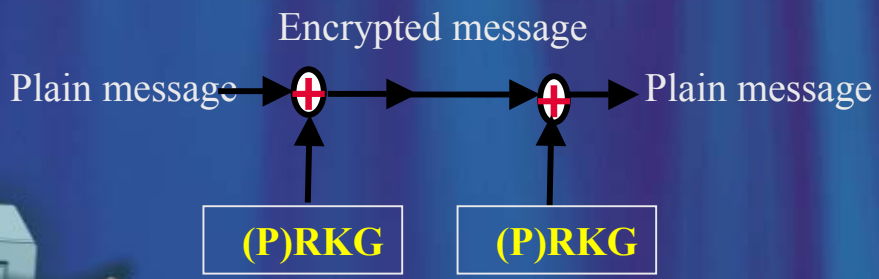
Block cipher
No internal state

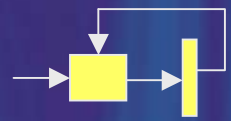


Stream ciphers
Internal state

Additive stream cipher
((Pseudo)random key generator
(P)RKG)

General stream cipher





Internal state evolution

Design criteria of block ciphers -1

- Estimated level of security vs. unconditioned security;
- Length of effective key K (128, 192 or 256 bits);
- Output is dependent of the complexity of cryptographic function;
- Confusion (use substitution) & diffusion (use transposition);
- Type of structure (Feistel structure etc.), type of operations;
- Number of rounds;
- ,,Good" substitution tables (S-box) and permutation tables (P-box);
- Algorithm for round key.

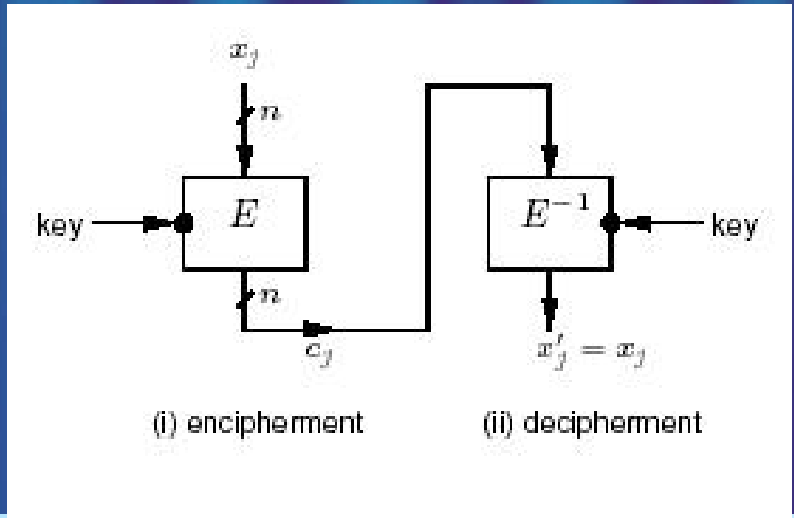
Design criteria of block ciphers -2

- Enciphering function vs. Deciphering function;
- Complexity of cryptographic function: hardware & software;
- Length of output block (usually 64, 128 or 256 bits);
- Text inflation: difference between length of plaintext length of cipher text;
- Error propagation.

Mode of operation of block cipher

- ECB (Electronic Code Book);
- CBC (Cipher Block Chaining);
- CFB (Cipher Feedback Block);
- OFB (Output Feedback Block);
- etc.

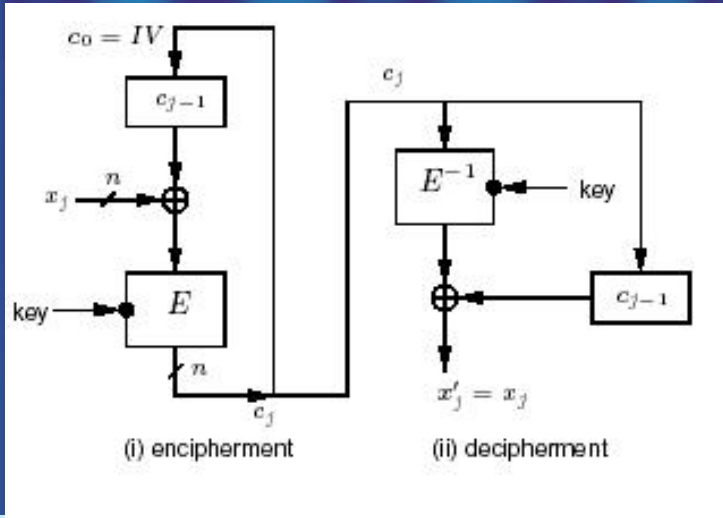
ECB (Electronic Code Book)



-Properties of the ECB mode of operation:

- Identical plaintext blocks (under the same key) result in identical ciphertext;
- Chaining dependencies: blocks are enciphered independently of other blocks. Reordering ciphertext blocks results in correspondingly re-ordered plaintext blocks;
- Error propagation: one or more bit errors in a single ciphertext block affect decipherment of that block only. For typical ciphers E, decryption of such a block is then random (with about 50% of the recovered plaintext bits in error);
- Since ciphertext blocks are independent, malicious substitution of ECB blocks (e.g., insertion of a frequently occurring block) does not affect the decryption of adjacent blocks. Furthermore, block ciphers do not hide data patterns – identical ciphertext blocks imply identical plaintext blocks. For this reason, the ECB mode is not recommended for messages longer than one block, or if keys are reused for more than a single one-block message. Security may be improved somewhat by inclusion of random padding bits in each block.

CBC (Cipher Block Chaining)



Properties of the CBC mode of operation:

- Identical plaintexts: identical ciphertext blocks result when the same plaintext is enciphered under the same key and *IV* . Changing the *IV* , key, or first plaintext block (e.g., using a counter or random field) results in different ciphertext;

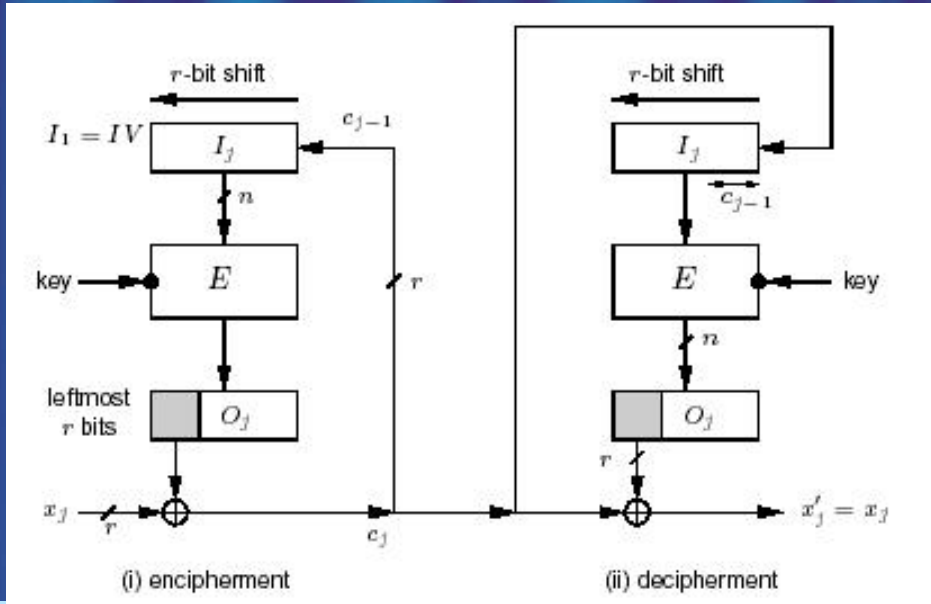
- Chaining dependencies: the chaining mechanism causes ciphertext c_j to depend on x_j and all preceding plaintext blocks (the entire dependency on preceding blocks is, however, contained in the value of the previous ciphertext block). Consequently, rearranging the order of ciphertext blocks affects decryption. Proper decryption of a correct ciphertext block requires a correct preceding ciphertext block;

CBC (Cipher Block Chaining) - cont

Properties of the CBC mode of operation:

- Error propagation: a single bit error in ciphertext block c_j affects decipherment of blocks c_j and c_{j+1} (since x_j depends on c_j and c_{j+1}). Block x_j' recovered from c_j is typically totally random (50% in error), while the recovered plaintext x_{j+1}' has bit errors precisely where c_j did. Thus an adversary may cause predictable bit changes in x_{j+1} by altering corresponding bits of c_j.
- Error recovery: the CBC mode is *self-synchronizing* or *ciphertext autokey* in the sense that if an error (including loss of one or more entire blocks)occurs in block c_j but not c_{j+1}, c_{j+2} is correctly decrypted to x_{j+2}.

CFB (Cipher Feedback Block)



Properties of the CFB mode of operation:

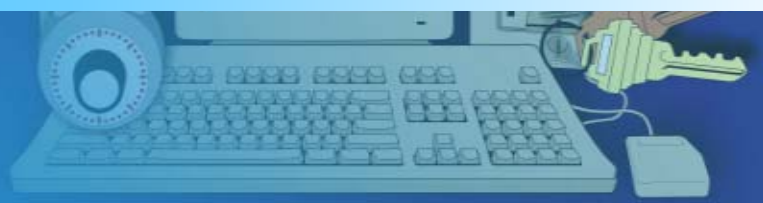
- Identical plaintexts: as per CBC encryption, changing the *IV* results in the same plaintext input being enciphered to a different output. The *IV* need not be secret (although an unpredictable *IV* may be desired in some applications);

- Chaining dependencies: similar to CBC encryption, the chaining mechanism causes ciphertext block c_j to depend on both x_j and preceding plaintext blocks; consequently, reordering ciphertext blocks affects decryption. Proper decryption of a correct ciphertext block requires the preceding [n/r] ciphertext blocks to be correct (so that the shift register contains the proper value);

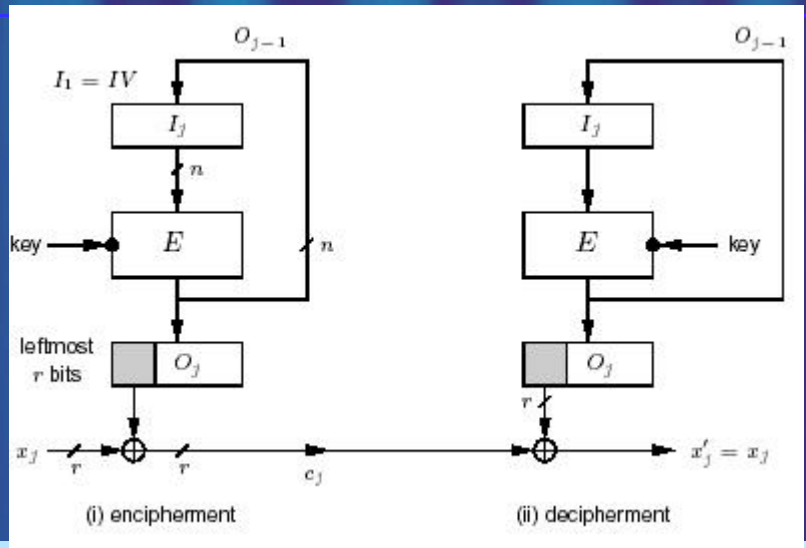
CFB (Cipher Feedback Block) - cont

Properties of the CFB mode of operation:

- Error propagation: one or more bit errors in any single r-bit ciphertext block c_j affects the decipherment of that and the next [n/r] ciphertext blocks (i.e., until n bits of ciphertext are processed, after which the error block c_j has shifted entirely out of the shift register). The recovered plaintext x_j' will differ from x_j precisely in the bit positions c_j was in error; the other incorrectly recovered plaintext blocks will typically be random vectors, i.e., have 50% of bits in error. Thus an adversarymay cause predictable bit changes in x_j by altering corresponding bits of c_j;
- Error recovery: the CFB mode is self-synchronizing similar to CBC, but requires [n/r] ciphertext blocks to recover;
- Throughput: for $r < n$, throughput is decreased by a factor of n/r (vs. CBC) in that each execution of *E* yields only r bits of ciphertext output.



OFB (Output Feedback Block)



Properties of the OFB mode of operation:

- Identical plaintexts: as per CBC and CFB modes, changing the *IV* results in the same plaintext being enciphered to a different output;
- Chaining dependencies: the keystream is plaintext-independent;
- Error propagation: one or more bit errors in any ciphertext character c_j affects the decipherment of only that character, in the precise bit position(s) c_j is in error, causing the corresponding recovered plaintext bit(s) to be complemented;
- Error recovery: the OFB mode recovers from ciphertext bit errors, but cannot self synchronize after loss of ciphertext bits, which destroys alignment of the decrypting keystream (in which case explicit re-synchronization is required);
- Throughput: for $r < n$, throughput is decreased as per the CFB mode. However, in all cases, since the keystream is independent of plaintext or ciphertext, it may be pre-computed (given the key and *IV*).

Evaluation, testing and cracking block ciphers

- Statistical methods: NIST IR (Interagency Reports) 6380 and 6483 using statistical test suite from NIST SP (Special Publication 800-22), DIEHARD etc;
- Classical attacks & side channel attacks;
- Attack on encryption key (brute force attack);
- Time space trade-offs:
    - Meet in the middle;
    - Hellman time – space trade off;
- Rainbow tables;
- Slide attacks;
- Linear cryptanalysis;
- Differential cryptanalysis, truncated differentials, impossible differentials, boomerang attacks, interpolation attacks, related key attacks etc.

Linear cryptanalysis - 1

Technique was introduced by Matsui si Yamagishi in 1991: *A new Method for known plain text attack of FEAL cipher* , Advances in Cryptology EUROCRYPT '92 Proceedings, Springer-Verlag, 1993, pp. 81-91;

Basically this technique finds a linear relationship (which holds in probability) between some bits from plaintext P, ciphertext C and key K which is used optimally in a second stage by finding the bits from the key that satisfies the linear relation and finally the rest of the bits using brute force for example;

Applied by:

M. Matsui, *Linear Cryptanalysis Method for DES Cipher*, Advances in Cryptology, EUROCRYPT '93 Proceedings, Springer-Verlag, 1994, pp. 386-397;

The First Experimental Cryptanalysis of the Data Encryption Standard, Advances in Cryptology, CRYPTO '94 Proceedings, Springer-Verlag, 1994, pp. 1-11.

K. Ohta si K. Aoki, *Linear Cryptanalysis of the Fast Data Encipherment Algorithm*, Advances in Cryptology, CRYPTO '94 Proceedings, Springer-Verlag, 1994, pp. 12-16.

Linear cryptanalysis - 2

Others references:

C. Harpes, G. C. Kramer and J. L. Massey, *A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-Up Lemma*, in Advances in Cryptology-EUROCRYPT'95. (Eds. L. C. Guillou and J.-J. Quisquater), Lecture Notes in Computer Science, No. 921. Heidelberg and New York: Springer, 1995, pp. 24-38.

C. Harpes, *Cryptanalysis of Iterated Block Ciphers*, ETH Series in Information Processing, Vol. 7 (Ed. J. L. Massey). Konstanz, Germany: Hartung-Gorre Verlag, 1996.

Z. Kukorelly, *On the Validity of Certain Hypotheses Used in Linear Cryptanalysis*, ETH Series in Information Processing, Vol. 13 (Ed. J. L. Massey). Konstanz, Germany: Hartung-Gorre Verlag, 1999.

Linear cryptanalysis - 3

Linear Cryptanalysis, introduced by Matsui at EUROCRYPT'93, is

- a **known-plaintext attack**
- on an iterated cipher (i.e., a block cipher in which a **"cryptographically weak" round function** is repeated *r* times)
- where one assumes that the known **plaintexts** had been chosen **independently and uniformly at random** (but it seems to work just as well no matter how the these plaintexts had been chosen)
- and one assumes that the **subkeys** used in the *r* "rounds" of encryption had been chosen **independently and uniformly at random** (but it seems to work just as well, or even better, if these subkeys were determined by a key schedule from a small random key).

Linear cryptanalysis - 4

The goal of linear cryptanalysis is to find the key that had been used for the encryption of all the known plaintexts, essentially by ***finding the key of the last round***.
Linear cryptanalysis usually requires such a **vast number of plaintext/ciphertext pairs** to be known in a successful attack that it is not a practical attack, but this required number is an excellent **measure of the cipher's lack of a linear weakness**.

Linear cryptanalysis - 5

The notion of the imbalance of a binary random variable plays a central role in linear cryptanalysis:

A binary random variable S is **balance** if $P(S = 0) = P(S = 1) = 1/2$.

The **imbalance** $I(S)$ of a binary random variable S is the real number:

$$I(S) = 2\,|P(S = 0) - ½|.$$

Note that $0 \le I(S) \le 1$ with equality on the left if and only if S is balanced, and with equality on the right if and only if S is a constant, i.e., $P(S = 0) = 1$ or $P(S = 0) = 0$.

The **conditional imbalance** of S given that $Z = z$ is the real number:

$$I(S \mid Z = z) = 2\,|P(S = 0 \mid Z = z) - ½|.$$

The **average-conditioned imbalance** of S given Z is the real number:

$$I(S \mid Z) = \Sigma z\, I(S \mid Z = z)\, P(Z = z)\ .$$

Average-conditioned imbalance plays an important role in linear cryptanalysis. The following simple fact explains many things:

Proposition: $I(S) \le I(S \mid Z)$ with equality if and only if the difference $P(S = 0 \mid Z = z) - 1/2$ has the same sign for all z with $P(Z = z) \neq 0$.

Linear cryptanalysis - 6

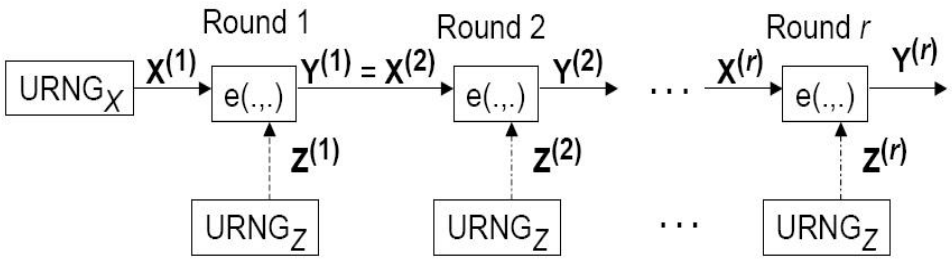
Two useful facts:

- For any binary constant b, $I(S \oplus b) = I(S)$.
- For any binary-valued function $h(.)$, $I(S \oplus h(Z) \mid Z = z) = I(S \mid Z = z)$.

Corollary to Proposition: For any binary valued function $h(.)$ of Z, $I(S \oplus h(Z)) \leq I(S \mid Z)$. Moreover, equality holds if and only if $h(.)$ is chosen so that the difference $P(S = h(z) \mid Z = z) - 1/2$ has the same sign for all z with $P(Z = z) > 0$.

Linear cryptanalysis – practical attack

Block cipher in r rounds, e(*,*) round encipher function, X plaintext (random generated), $X^{(i)}$ input in round *i*, $Y^{(i)}$ output from round i, $Z^{(i)}$ key in round *i*:



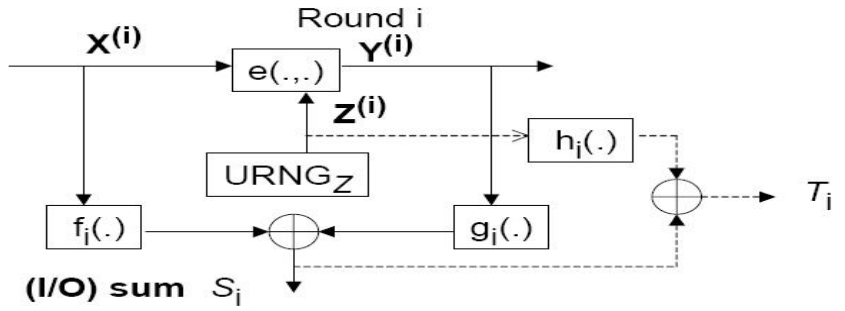
STEP 1. Find an (*r*-1)-round I/O sum $S_{1...(r-1)} = f_1(\mathbf{X^{(1)}}) + g_{r-1}(\mathbf{Y^{(r-1)}})$ with ,,large" imbalance;

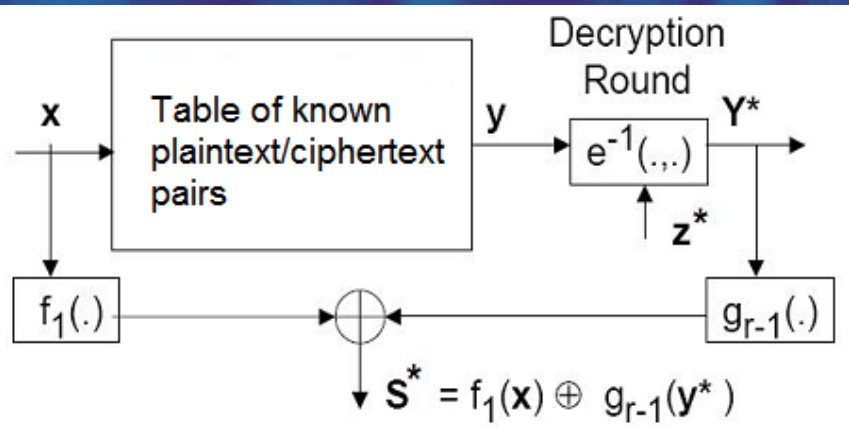
STEP 2. For each value **z*** of the subkey in round *r* (or more precisely of those bits of this key that affect the value of g_{r-1} (**y***)):

- for each plaintext **x**, decrypt the corresponding ciphertext **y** for only one round of decryption to obtain **y***;
- compute the value $\mathbf{S^*} = f_1(\mathbf{x}) + g_{r-1}(\mathbf{y^*})$, which is the value of $S_{1...(r-1)}$ assuming that the key was guessed correctly;
- compute the empirical imbalance of these values;

STEP 3. Decide on the key **z*** that gave the greatest empirical imbalance.

In each round *i* we compute the sum S_i between input and output and also the sum T_i. Functions $f_i(.)$, $g_i(i)$ are balanced and $h_i(.)$ is arbitrary (this is a **generalization** of the approach of Matsui, who required that the functions fi(.), gi(.) and hi(.) are be **linear** functions, i.e., modulo-two sums of their input variables):





Linear cryptanalysis – why attacks works

Matsui's "Piling-Up Lemma: If T_1, T_2, …, T_n are independent binary-valued random variables, then $\mathrm{I}(T_1 \oplus T_2 \oplus \ldots \oplus T_n) = \mathrm{I}(T_1) \bullet \mathrm{I}(T_2) \bullet \ldots \bullet \mathrm{I}(T_n)$.
This lemma suggests that the imbalance $\mathrm{I}(T_1 \oplus T_2 \oplus \ldots \oplus T_n)$ will decrease rapidly as n increases, even when one has made the best choice of T_1, T_2, …, T_n.
The difficult problem in linear cryptanalysis is finding the (r-1)-round I/O sum with (the) large(est) average-conditioned imbalance $\mathrm{I}(S_{1\ldots(r\text{-}1)} \mid Z_{r\text{-}1})$ to use in the attack.

Linear cryptanalysis – others facts

It is important to remember

• that in the actual attack by linear cryptanalysis, one uses only the parent I/O sum, not the threefold sums used to find this I/O sum,

• that in particular one never makes use of the key functions $h(\mathbf{Z}_i)$ of these threefold sums except in the sense that the better one picks these functions the closer the computed (or estimated) imbalance, $I(S \oplus h(\mathbf{Z}))$, will be to the imbalance $I(S \mid \mathbf{Z})$ that governs the success of the attack, and

• **the attack will usually work better than predicted** from the value of $I(S \oplus h(\mathbf{Z}))$ since it is not likely that one will have found the absolutely best h(.).

Linear cryptanalysis has proved to be very effective (usually better than differential cryptanalysis) against ciphers (such as DES and FEAL) where the key is inserted into the round by bit-by-bit modulo two addition

Linear cryptanalysis has not been successful against ciphers where the key is inserted into the round by a modular addition for large moduli.

Differential cryptanalysis

Technique introduced by Biham & Schamir in ,,Diferential Cryptanalysis of the Data Encryption Standard", Springer-Verlag, 1993;

Belongs to the class of chosen plaintext attacks: given the pair (D,D'), called characteristics, the method consists in generation of plaintext pairs (P_1,P_2) with $D=P_1 - P_2$ such that $D'=C_1-C_2$ and find a part of a key and after that using brute force searching for find the rest of the key;

Operation ,,-" is group operation which, for example in case of block ciphers, consist in adding the round key;

Differential cryptanalysis was applied by:

S. Murphy, ,,The Cryptanalysis of FEAL-4 with 20 Chosen Plaintexts" (Journal of Cryptology, V. 2, N. 3, 1990, pp. 145-154;

L. Brown, J. Pieprzyk si J. Seberry, ,,LOKI: A Cryptographic Primitive for Authentication and Secrecy Applications", Advances in Cryptology - AUSCRYPT '90 Proceedings, Springer-Verlag, 1990, pp. 229-236;

X. Lai si J. Massey, ,,A Proposal for a New Block Encryption Standard", Advances in Cryptology - EUROCRYPT '90 Proceedings, Springer- Verlag, 1991, pp. 389-404;

E. Biham si A. Shamir, ,,Diferential Cryptanalysis of Snefru, Khafre, REDOC II, LOKI, and Lucifer", Advances in Cryptology - CRYPTO '91 Proceedings, Springer-Verlag, 1992, pp. 156 -171.

Differential cryptanalysis models

Classical differential cryptanalysis;

Truncated differential cryptanalysis;

Impossible differential cryptanalysis;

Higher order differential cryptanalysis (boomerang attack);

Differential – linear cryptanalysis;

Interpolation attack;

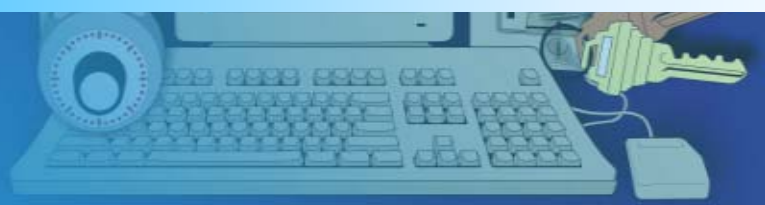
Related key attack.

Classical differential cryptanalysis -1

Differential Cryptanalysis, introduced by Biham and Shamir at CRYPTO'90, is:

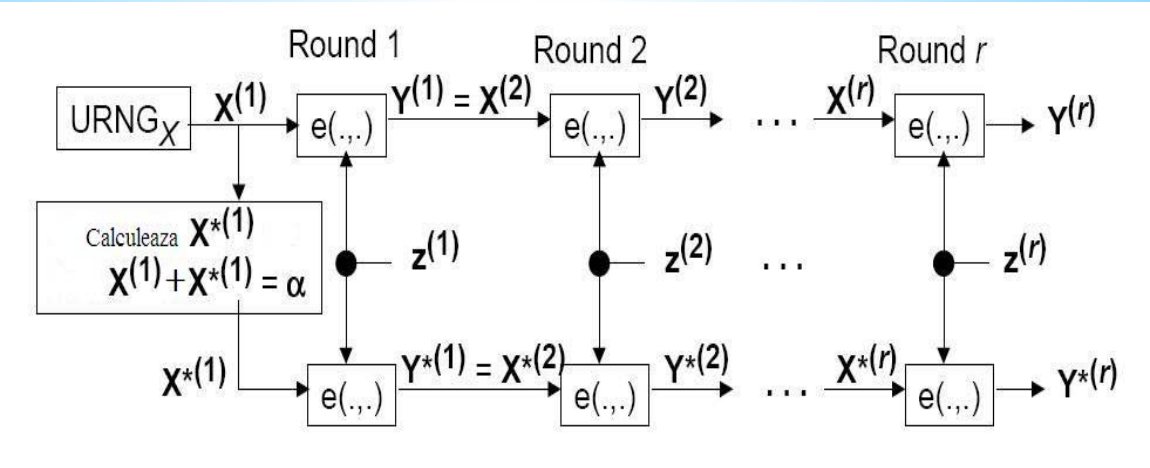
- a **chosen-plaintext attack**
- on an iterated cipher (i.e., a block cipher in which a **"cryptographically weak" round function** is repeated *r* times)
- where one assumes that the **subkeys** used in the *r* "rounds" of encryption are chosen **independently and uniformly at random** (but it seems to work just as well, or even better, if these subkeys were determined by a key schedule from a small random key).

The goal of differential cryptanalysis is to find the key that had been used for the encryption of all the chosen plaintexts, essentially by ***finding the key of the last round***. Differential cryptanalysis usually requires such a **vast number of plaintext/ciphertext pairs** to be known in a successful attack that it is not a practical attack, but this required number is an excellent **measure of the cipher's security against "differential" weaknesses**.



Classical differential cryptanalysis - 2

Classical differential cryptanalysis: using pair of plaintext/cipertext and the differentials we find the last round key;



For the differential (α, β) in round (r -1):
STEP 1. Randomly choose a plaintext **X(1)** and compute **X*(1)** so that Δ**X(1) = X(1) + X*(1)** = α . Encrypt **X(1)** and **X*(1)**.
STEP 2. Assuming that Δ**Y(r-1)** = β, find all values of the subkey **z(r)** consistent with Δ**Y(r-1)** and the obtained ciphertexts **Y(r)** and **Y*(r)**. Add 1 to the "occurrence count" for these subkeys.
STEP 3. Repeat (1) and (2) until some key is counted significantly more often than the others. Announce this subkey **z(r)** as the decision for the last-round subkey..

Classical differential cryptanalysis - 3

As was pointed out by Lai, Massey & Murphy, the theory of differential cryptanalysis rests on the:

Hypothesis of Stochastic Equivalence:

$P[\Delta \mathbf{Y}^{(i)} = \beta \mid \Delta\, \mathbf{X}^{(1)} = \alpha]$ has approximately the same value in both the "attack" model and the "analyzed" model for virtually all keys $\mathbf{z}^{(1)}$, $\mathbf{z}^{(2)}$, … $\mathbf{z}^{(r)}$ (generated by a (P)RG);

One uses the "analyzed" model to compute the probabilities that are then used in the attack:

The success of differential cryptanalysis depends on being able to find an ***(r -1)-round differential*** (α, β) such that $P[\Delta\, \mathbf{Y}^{(r-1)} = \beta \mid \Delta\, \mathbf{X}^{(1)}) = \alpha] >> 2^{-N}$.

Truncated differential cryptanalysis

In case of a block cipher (with r-rounds) characteristics is the array (D_0, D_1,…,D_{r-1}) with $D=D_0$ si $D_{r-1}=D'$;

Truncated characteristic: study a part from the characteristics array (D_0, D_1,…,D_{r-1});

Difference between characteristics and differentials: X. Lai, J. L. Massey, and S. Murphy, ,,Markov ciphers and differential cryptanalysis", Proceedings of Eurocrypt'91 (D. W. Davies, ed.), no. 547 in Lecture Notes in Computer Science, pp. 17–38, Springer-Verlag, 1991. In fact differentials have assigned a probability of occurrence.

Truncated differential cryptanalysis was applied by L.R. Knudsen in

,,Truncated and Higher Order Differentials", Fast Software Encryption, 2nd International Workshop Proceedings, Springer-Verlag, 1995, pp. 196- 211;

,,Truncated Differentials of SAFER Fast Software Encryption", 3rd International Workshop Proceedings, Springer-Verlag, 1996, pp. 15-26.

Impossible differential cryptanalysis

Impossible differentials: study of those characteristics (D_0, D_1,…,D_{r-1}) which occur with probability 0. Technique was described in:

Knudsen, ,,DEAL - a 128-bit block cipher", Technical report 151, Dept. of Informatics, University of Bergen, Norway, 1998;

E. Biham, A. Biryukov and A. Shamir, ,,Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials", Proceedings of Eurocrypt'99.

Higher order differential cryptanalysis

Higher order differentials consist in recursive application of the differential. For example boomerang attack (Wagner) is a application of the differential cryptanalysis of order 2 in which first order differential is applied at the first part of the cipher and the differential of second order is applied at the second part of the cipher. Technique was presented in:

X. Lai, ,,Higher Order Derivatives and Diferential Cryptanalysis“, Communications and Cryptograpy, Kluwer Academic Publishers, 1994,pp. 227-233;

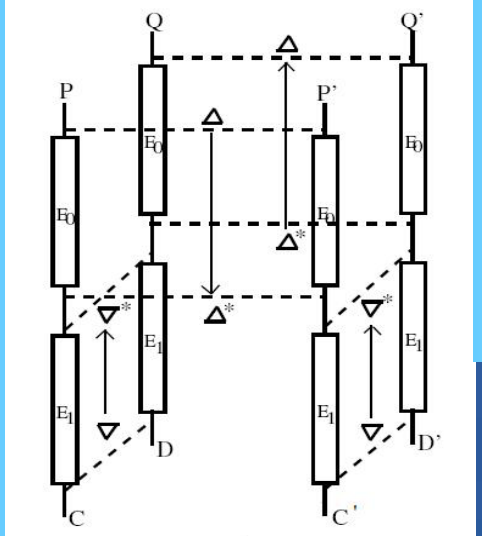
L.R. Knudsen, ,,Truncated and Higher Order Diferentials“, Fast Software Encryption, 2nd International Workshop Proceedings, Springer-Verlag, 1995, pp. 196-211.

Boomerang attack: involve pairs of plaintext (P,P') with the differential characteristics (Δ,Δ^*) for E_0 and also pairs of plaintext (P,Q) si (P',Q') with differential characteristics (∇,∇^*) for E_1^{-1}.

Pair (Q, Q') can be used for definiting the characteristc $\Delta^* \rightarrow \Delta$ for E_0^{-1}:

$E_0(Q) \oplus E_0(Q') = E_0(P) \oplus E_0(P') \oplus E_0(P) \oplus E_0(Q) \oplus E_0(P') \oplus E_0(Q') = E_0(P) \oplus E_0(P') \oplus E_1^{-1}(C) \oplus E_1^{-1}(D) \oplus E_1^{-1}(C') \oplus E_1^{-1}(D') = \Delta^* \oplus \nabla^* \oplus \nabla^* = \Delta^*$;

We have the same characteristics between Q and Q' like between P and P';



Qvartet setting:

generate (choosen plaintext attack) P'=P⊕Δ obtain C and C';

generate (adaptive plaintext attack) D=C⊕∇ si D'=C'⊕∇;

decrypt D and D' for obtaining Q and Q'.

Diferential – linear cryptanalysis

Differential – linear cryptanalysis is a hybrid method which use differential and linear cryptanalysis.
The trick is to use a linear expression, developed in a way already shown, and to measure what changes in the plaintext do to the value of that linear expression. In this way, we aren't simply brute-forcing the subkeys by calculating counts on the linear expression; rather, we are using carefully selected differentials that should produce fixed, expected probabilities of the linear expressions being XORed being equal to 0. As before, we normally expect this to happen roughly half the time for any arbitrary linear expressions and difference; thus any deviation from this can be used.

Example: AES – FIPS 107

(Advanced Encryption Standard)

- Was the result of a public competition organized by NIST;

- RIJNDAEL (designed by Joan Daemen and Vincent Rijmen) block cipher with variable key length and variable block length;

- AES is RIJNDAEL with 128 data bits and 128, 192 or 256 key bits;

- AES is standardized in FIPS 197;

- Certified by National Security Agency for protection up to level **SECRET** (128 key bits) respectively **TOP SECRET** (192 or 256 key bits).

References

1. Menenzes A.J., et. al., Handbook of Applied Cryptography, CRC Press, 1997.
2. Schneier B., Applied Cryptography, John Wiley & Sons Inc., 1998.
3. Simion E., Preda V., Popescu A., Criptanaliza. Rezultate si Tehnici Matematice, Ed. Universitatii Bucuresti, 2004.
4. Simion E., Stream ciphers, Lectures notes, 2008.
5. Simion E., Block ciphers, Lectures notes, 2007.
6. Simion E., Statistical-informational analysis, Lectures notes, 2008.
7. Stallings W., Cryptography and Network Security: Principles and Practice, Prentice Hall, Second Edition, 1999.
8. Tilborg, Henk C.A. van, Fundamentals of Cryptology, Kluwer Academic Publisher, Second Edition, 2001.

Questions and Answers