A Brief Outlook at Block Ciphers

Pascal Junod

LASEC

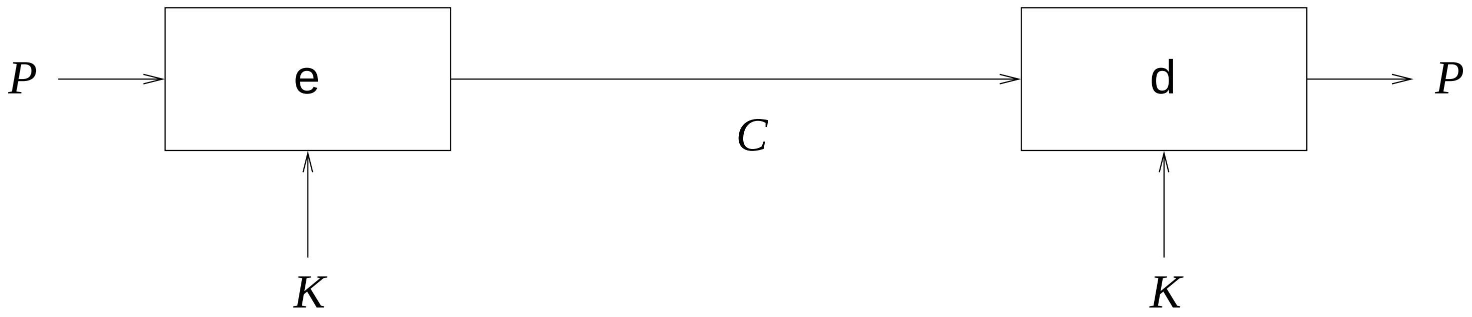
École Polytechnique Fédérale de Lausanne, Suisse

CSA'03, Rabat, Maroc, 10-09-2003

Content

- Generic Concepts
- DES / AES
- Cryptanalysis of Block Ciphers
- Provable Security

Block Cipher



Block Cipher (2)

★ Deterministic, invertible function:

$$\begin{aligned} \mathsf{e} : \{0,1\}^n \times \mathcal{K} &\rightarrow \{0,1\}^n \\ \mathsf{d} : \{0,1\}^n \times \mathcal{K} &\rightarrow \{0,1\}^n \end{aligned}$$

★ The function is parametered by a *key* K.

★ Mapping an n-bit *plaintext* P to an n-bit *ciphertext* C:

$$C = \mathsf{e}_K(P)$$

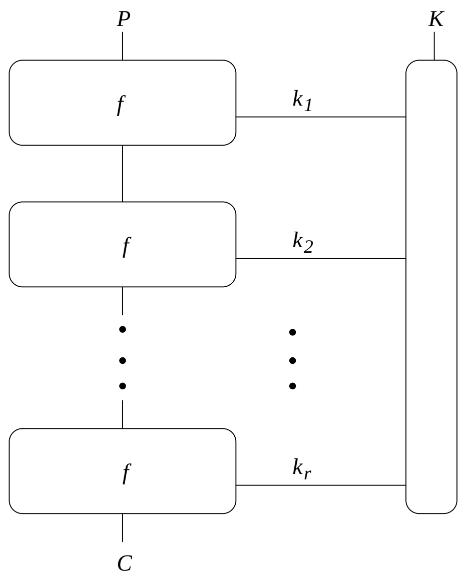
★ The function must be a *bijection* for a fixed key.

Product Ciphers and Iterated Block Ciphers

- A *product cipher* combines two or more transformations in a manner intending that the resulting cipher is (hopefully) more secure than the individual components.

- An *iterated block cipher* is a block cipher involving the sequential repetition of an internal function f called a *round function*. Parameters include the number of rounds r, the block bit size n and the bit size k of the input key K from which r *subkeys* k_i (called *round keys*) are derived. For invertibility purposes, the round function f is a bijection on the round input for each value k_i.

Product Ciphers and Iterated Block Ciphers (2)



Good and Bad Block Ciphers

★ Flexibility

★ Throughput

★ Estimated Security Level

Data Encryption Standard (DES)

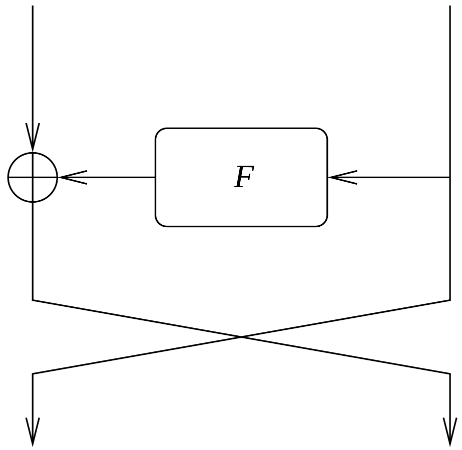
★ American standard from (1976 - 1998).

★ Designed by a team of IBM.

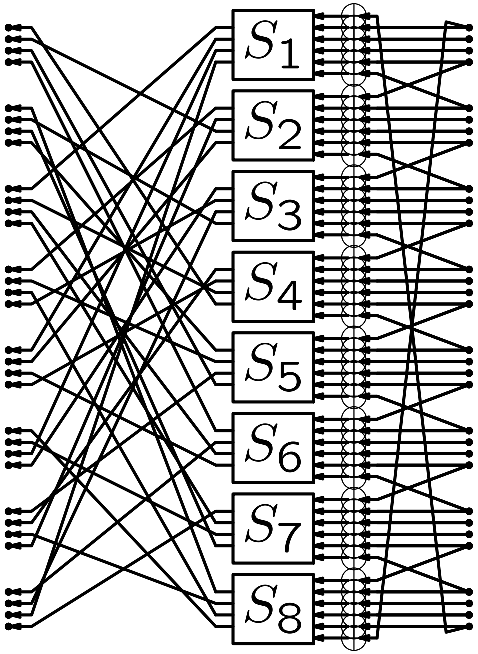
★ Iterated block cipher with 64-bit block size, 56-bit key size.

★ High-level structure is a *Feistel scheme*.

Feistel Scheme



DES f-Function



Advanced Encryption Standard (AES)

- Competitive basis
- 15 candidates
- 5 finalists: Rijndael, Serpent, Twofish, Mars, RC6
- Rijndael has become the AES
- Encrypts 128-bit blocks under 128-, 192- and 256-bit keys.

AES

★ Substitution-Permutation Network

★ Write the data as a 4×4 matrix over elements of GF(2^8):

$$\begin{array}{cccc} x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} \\ x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} \\ x_{3,1} & x_{3,2} & x_{3,3} & x_{3,4} \\ x_{4,1} & x_{4,2} & x_{4,3} & x_{4,4} \end{array}$$

★ 4 main operations: key addition, SubBytes, ShiftRows, MixColumns

AES (2)

- 10 - 14 rounds (depends on the key length)
- SubBytes: inversion operation in $GF(2^8)$ followed by an affine application on $GF(2)^8$.
- MixColumns: linear (4, 4)-multipermutation on $GF(2^8)^4$.
- ShiftRows: row-wise rotation of the matrix components.

AES (3)

★ Plus de détails sur AES lors des "travaux pratiques" de demain !

Speed

Name	Key Size	Cycles / byte on an Intel P3
RC5	64	19
CAST-128	128	30
Nimbus	128	34
Khazad	128	39
Hierocrypt	128	43
Nush	128	44
Misty1	128	47
IDEA	128	55
DES	56	59
KASUMI	128	73
Skipjack	80	114
SAFER++	128	152
Triple-DES	168	154
CS-Cipher	128	156

Speed (2)

Name	Key Size	Cycles / byte on an Intel P3
RC6	256	18
Nush	256	23
Twofish	256	28
Mars	256	31
AES	256	32
SC2000	256	43
Camellia	256	45
Anubis	256	47
Serpent	256	59
SAFER++	256	63
Hierocrypt	256	67

Kerkhoffs' Principle

The adversary knows all details of the encrypting and decrypting processes, except for the value of the secret key.

Attack Models

★ Global Deduction

★ Local Deduction

★ Information Deduction

★ Distinguishing Attack

Attack Scenarii

- ★ Ciphertext-Only Attack
- ★ Known-Plaintext Attack
- ★ Chosen-Plaintext Attack
- ★ Non-Adaptive *vs.* Adaptive Attacks

Generic Attacks

- Exhaustive Key Search (related to the key size)
- Ciphertext-Matching Attack (related to the block size)
- Hellman's Time-Memory Tradeoff

Differential Cryptanalysis

★ Chosen-plaintext attack (re-) discovered by Biham and Shamir (1990).

★ Looks at ciphertext pairs whose corresponding plaintexts have a particular difference: $(P, P + \Delta) \rightarrow (C, C + \Delta')$.

★ Last-round attack concept.

Differential Cryptanalysis (2)

★ Since then, many variants have been described.

★ Truncated, impossible, high-order differential cryptanalysis.

★ Boomerang attack, rectangle attack

Linear Cryptanalysis

- ★ Invented by Matsui in 1993, based on ideas of Gilbert *et al.*.
- ★ Known-plaintext attack.
- ★ Looks at equation of the type

$$\mathbf{a} \cdot P \oplus \mathbf{b} \cdot C = \mathbf{c} \cdot K$$

- ★ One expects that the above equation is probabilistically "biased".

Other Attacks

★ Differential-Linear Cryptanalysis

★ Integral Cryptanalysis

★ Interpolation Attack

★ Statistical Attacks

Algebraic Attacks

- ★ Shannon (1949) stated that the break of a block cipher should "*require as much work as solving a system of simultaneous equations in a large number of unknowns of a complex type*".
- ★ Overdefined systems (AES) (papers of Courtois, Pieprzyk, Murphy, Robshaw...)
- ★ Actual (real) complexity of the known solving algorithms remains at this time an open problem.
- ★ Ongoing, exciting research field !

Attacks against the Key-Schedule Algorithm

★ Linear Factors

★ Related-Key Attacks

★ Slide Attacks

★ Weak Keys

Provable Security

- ★ Theoretical Notions of Security
- ★ Linear, Differential Cryptanalysis
- ★ Luby-Rackoff Model
- ★ Decorrelation Theory

Luby-Rackoff Model

- Distinguisher δ: computationally unbounded Turing machine.
- Oracle Ω implements a permutation on $\{0,1\}^n$.
- C *vs.* C^*
- The distinguisher can submit a bounded number of queries to Ω and ultimately outputs a decision bit.

Luby-Rackoff Model (2)

★ Advantage:

$$\mathsf{Adv}^n_\delta(C, C^*) = \left| \Pr_C [\delta(\mathbf{x}) = 1] - \Pr_{C^*} [\delta(\mathbf{x}) = 1] \right|$$

★ Best Advantage

$$\mathsf{BestAdv}^n(C, C^*) = \max_\delta \mathsf{Adv}^n_\delta(C, C^*)$$

★ A "security proof" means that one is able to provide an acceptable *upper bound* on $\mathsf{BestAdv}^n(C, C^*)$ for a given block cipher C.

Luby-Rackoff Model (3)

★ Feistel scheme is the most studied one in the Luby-Rackoff model.

★ For 4 rounds or more, a random Feistel scheme is secure against *known-plaintext* attacks.

★ For 7 rounds or more, a random Feistel scheme is secure against *chosen-plaintext* attacks.

★ For 10 rounds or more, a random Feistel scheme is secure against chosen-plaintext *and* chosen-ciphertext attacks.

Decorrelation Theory

- ★ Constructive *Security Framework* proposed by Vaudenay (1998).
- ★ Based on the Luby-Rackoff model.
- ★ Central concept is the *decorrelation matrix of order d* of a random function F:

$$[F]^d_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)} = \Pr_K[F(x_1) = y_1 \wedge \ldots \wedge F(x_d) = y_d]$$

Decorrelation Theory (2)

★ Given the decorrelation matrix of a random function F, one can compare it to a *canonical function* F^* using the concept of *decorrelation bias*:

$$\mathsf{Dec}^d(F) = ||\,[F]^d_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)} - [F^*]^d_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)}\,||$$

★ Idea: find a matrix distance meaning something in terms of "security"!

★ Link to the best advantage of any adaptive distinguisher limited to d queries through the following distance:

$$||M||_a \triangleq \max_{x_1}\sum_{y_1}\max_{x_2}\sum_{y_2}\cdots\max_{x_d}\sum_{y_d}|M_{(x_1,\ldots,x_d)(y_1,\ldots,y_d)}|$$

Decorrelation Theory (3)

Theorem 1

$$\mathsf{BestAdv}^d(F,F^*) = \frac{1}{2}\cdot\left|\left|\,[F]^d_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)} - [F^*]^d_{(x_1,\ldots,x_d),(y_1,\ldots,y_d)}\,\right|\right|_a$$

Decorrelation Theory (4)

- Concept of decorrelation modules.
- DFC, candidate for the AES contest.

Future Perspectives

- ★ New designs, new attacks.
- ★ Study of generic attacks.
- ★ Provable security for block ciphers !?

Related Topics

- Stream Ciphers
- Modes of Encryption
- Combined primitives (confidentiality + authentication)

More Information

- `http://csrc.nist.gov/CryptoToolkit/aes/`
- `http://www.cryptonessie.org`
- Proceedings of Crypto, Eurocrypt, Asiacrypt, Fast Software Encryption (FSE), Selected Areas in Cryptography (SAC), and other conferences published in Springer's Lecture Notes in Computer Science.

Merci !

Email: `pascal@junod.info`

Homepage: `http://crypto.junod.info`

Homepage of my lab: `http://lasecwww.epfl.ch`

Questions ?