

MODERN CRYPTOGRAPHY FOR INFORMATION SECURITY APPING2: [Level I]

cryptoing2@gmail.com

December 2018 — Symmetric Cryptography

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

- ➊ Symmetric modern Ciphers
- ➋ Block cipher modes of operation
- ➌ Confusion and Diffusion
- ➍ DES, 2DES & 3DES
- ➎ Other remarks about DES
- ➏ AES/Rijndael
- ➐ Cryptographic Hash Functions
- ➑ The Hash Function MD4 (simplified)
- ➒ SHA-1 (short version)
- ➓ Hash functions : Uses
- ➔ Attacks of SHA-0
- ➕ The future : SHA-3?

① Symmetric modern Ciphers

Definitions [WIK, Sti10, MvOV97]

- Symmetric-key algorithms are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both decryption and encryption.
- The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Definitions [WIK, Sti10, MvOV97]

Other terms for symmetric-key encryption are :

- ① secret-key,
- ② single-key,
- ③ one-key
- ④ and sometimes *classical encryption* or also *private-key encryption*.

Use of the latter term does conflict with the term private key in public key cryptography.

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

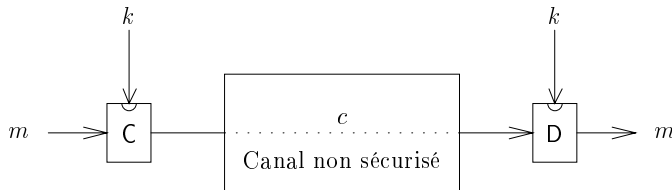
The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Secured channel with symmetric cipher : we use an unsecured channel



Types of symmetric cypher : Symmetric-key algorithms

...

... are divided into **stream** and **block** ciphers :

- Stream ciphers encrypt the bits of the message one at a time, and block ciphers take a number of bits and encrypt them as a single unit.
- Blocks of 64 bits are commonly used till 2000
- but now the AES algorithm (*aka* **Rijndael**) approved by NIST (2001) uses 128-bit blocks (or 196 or 256-bit blocks).

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Some examples of popular and well-respected symmetric algorithms include :

Finalists from AES NIST/DOD Contest, all are block ciphers :

- AES : ex *Rijndael* : chosen as AES October 2, 2000
- MARS (Finalist)
- RC6 (Finalist)
- Serpent (Finalist)
- Twofish (Finalist)
- nDES : DES (dead), 2DES (*deprecated/obsolete*) & 3DES (still *alive*)
- IDEA
- FORTEZZA : developed for the U.S. government's Clipper chip project : try don't use it!

Speed and Key management

- 1 Symmetric-key algorithms are generally much less computationally intensive than asymmetric key algorithms. In practice, asymmetric key algorithms are typically hundreds to thousands times slower than symmetric key algorithms.
- 2 One disadvantage of symmetric-key algorithms is the requirement of a shared secret key, with one copy at each end. To limit the impact of a potential discovery by a cryptographic adversary, they should be changed regularly and kept secure during distribution and in service. The process of selecting, distributing and storing keys is known as **key management**; it is difficult to achieve reliably and securely.

② Block cipher modes of operation

Block cipher modes of operation

- In cryptography, a block cipher operates on blocks of fixed length, often 64 or 128 bits,
- But now also 196 or 256 bits
- Because messages may be of any length, and because encrypting the same plaintext under the same key always produces the same output (as described in the ECB section below), several modes of operation have been invented which allow block ciphers to provide confidentiality for messages of arbitrary length

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

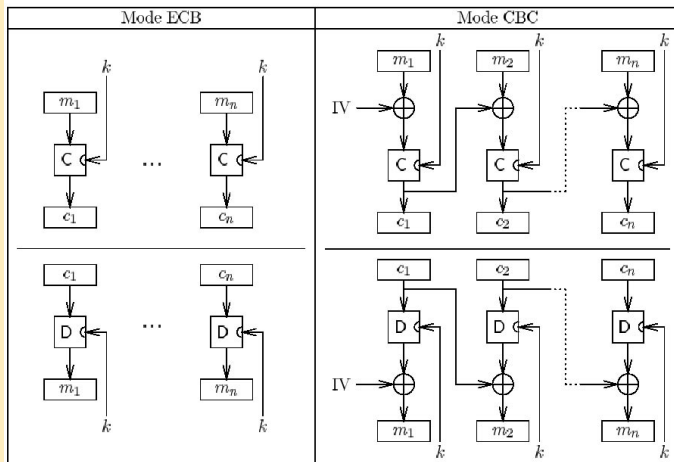
Block cipher modes of operation

The earliest modes described in the literature are :

- ① ECB
- ② CBC
- ③ OFB
- ④ CFB
- ⑤ + Counter mode

provide only confidentiality or message integrity, but do not perform both simultaneously. Other modes have since been designed which ensure both confidentiality and message integrity in one pass, such as IAPM, CCM, EAX, GCM, and OCB modes.

Some block cipher modes of operation



Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

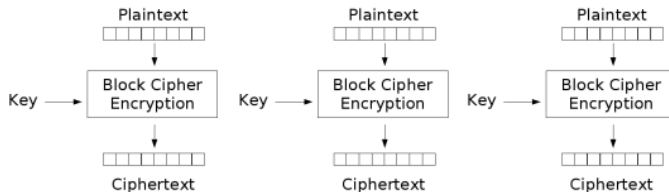
The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Electronic codebook (ECB) encryption mode of operation/WIKIPEDIA



Electronic Codebook (ECB) mode encryption

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

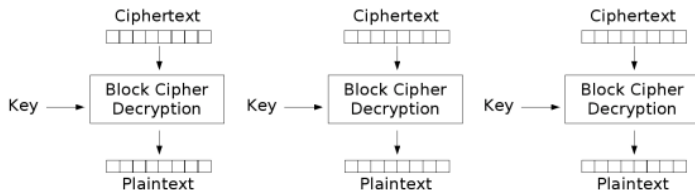
The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Electronic codebook (ECB) decryption mode of operation



Electronic Codebook (ECB) mode decryption

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

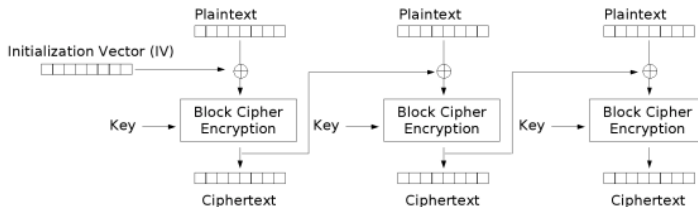
Cipher-block chaining (CBC) mode of operation

IV=Initialization Vector

$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$$

$$P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV$$

Cipher-block chaining (CBC) encryption mode of operation



Cipher Block Chaining (CBC) mode encryption

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

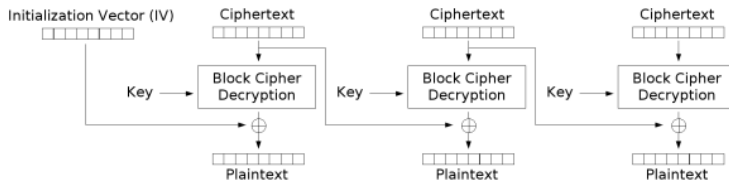
The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Cipher-block chaining (CBC) decryption mode of operation



Cipher Block Chaining (CBC) mode decryption

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Cipher feedback (CFB) encryption mode

The cipher feedback (CFB) mode, a close relative of CBC, makes a block cipher into a self-synchronizing stream cipher. Operation is very similar; in particular, CFB decryption is almost identical to CBC encryption performed in reverse :

$$C_i = E_K(C_{i-1}) \oplus P_i$$

$$P_i = E_K(C_{i-1}) \oplus C_i$$

$$C_0 = IV$$

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

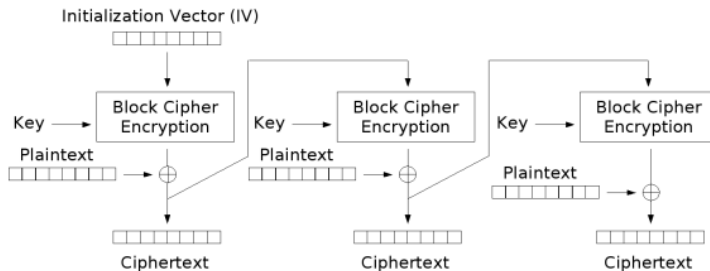
The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Cipher feedback (CFB) encryption mode



Cipher Feedback (CFB) mode encryption

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

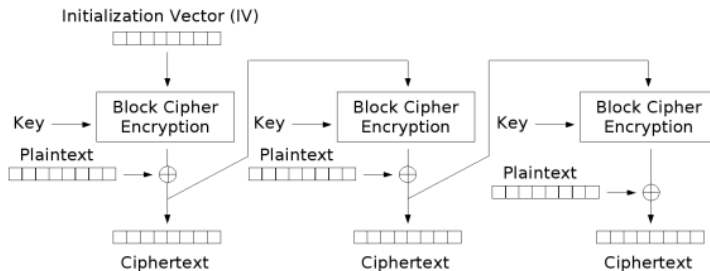
The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Cipher feedback (CFB) decryption mode



Cipher Feedback (CFB) mode encryption

Output feedback mode (OFB)

The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher : it generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error correcting codes to function normally even when applied before encryption.

Because of the symmetry of the XOR operation, encryption and decryption are exactly the same :

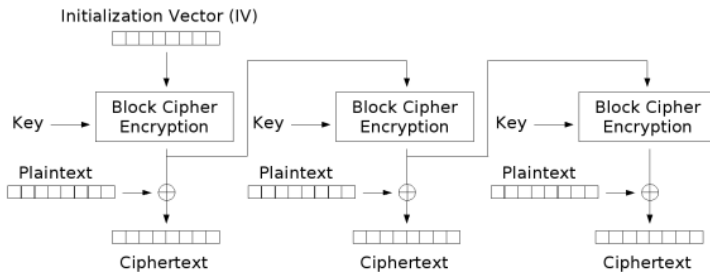
$$C_i = P_i \oplus O_i$$

$$P_i = C_i \oplus O_i$$

$$O_i = E_K(O_{i-1})$$

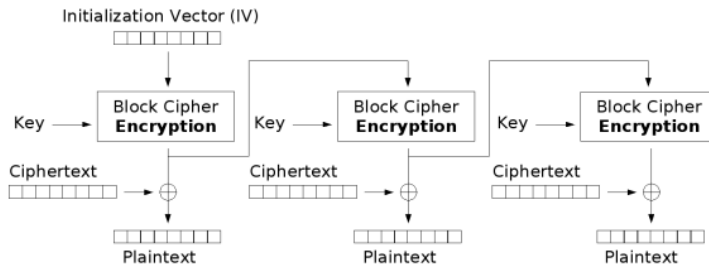
$$O_0 = IV$$

Output feedback encryption mode (OFB)



Output Feedback (OFB) mode encryption

Output feedback decryption mode (OFB)



Output Feedback (OFB) mode decryption

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

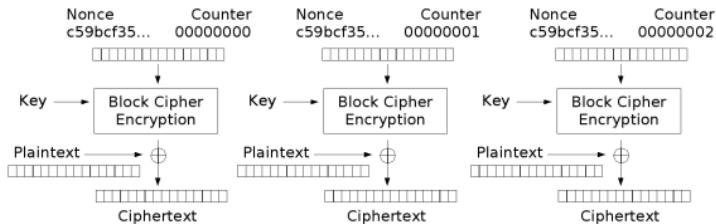
Hash functions :
Uses

Attacks of SHA-0

Another mode : Counter mode (CTR)

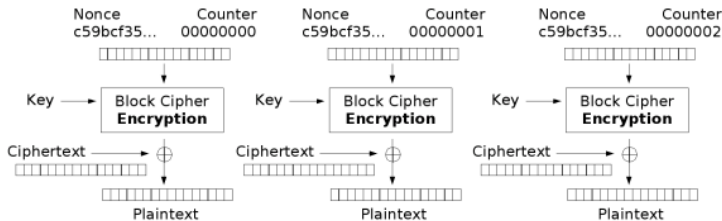
Like OFB, counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter". The counter can be any simple function which produces a sequence which is guaranteed not to repeat for a long time, although an actual counter is the simplest and most popular. CTR mode has similar characteristics to OFB, but also allows a random access property during decryption. Note that the nonce in this graph is the same thing as the initialization vector (IV) in the other graphs. The IV/nonce and the counter can be concatenated, added, or XORed together to produce the actual unique counter block for encryption. CTR mode is well suited to operation on a multi-processor machine where blocks can be encrypted in parallel.

Counter encryption mode (CTR)



Counter (CTR) mode encryption

Counter decryption mode (CTR)



Counter (CTR) mode decryption

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Example : a picture (WIKIPEDIA)



Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Example (following) : Picture encrypted in the ECB mode



EPITA -
Cryptography

R. ERRA

Symmetric modern
Ciphers

**Block cipher
modes of
operation**

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

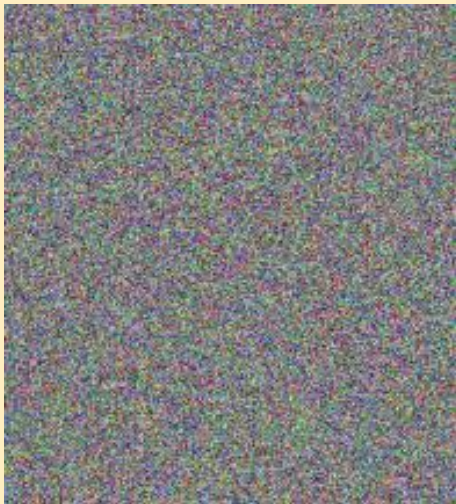
The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Example (following) : Picture encrypted in a different mode



EPITA -
Cryptography

R. ERRA

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

EPITA -
Cryptography

R. ERRA

Symmetric modern
Ciphers

Block cipher
modes of
operation

**Confusion and
Diffusion**

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

③ Confusion and Diffusion

Confusion et Diffusion : Shannon's work

In cryptography, confusion and diffusion are two properties of the operation of a secure cipher which were identified by Shannon in his paper, "Communication Theory of Secrecy Systems" published in 1949.

- ① **Confusion** : refers to making the relationship between the key and the ciphertext as complex and involved as possible ; diffusion refers to the property that redundancy in the statistics of the plaintext is "dissipated" in the statistics of the ciphertext.
- ② **Diffusion** : associated with dependency of bits of the output on bits of the input. In a cipher with good diffusion, flipping an input bit should change each output bit with a probability of one half (this is termed the Strict Avalanche Criterion).

Remarks

- Substitution (a plaintext symbol is replaced by another) has been identified as a mechanism for primarily confusion (see S-box);
- conversely transposition (rearranging the order of symbols) is a technique for diffusion, although other mechanisms are also used in modern practice, such as linear transformations (e.g. in Rijndael).
- Product ciphers use alternating substitution and transposition phases to achieve both confusion and diffusion respectively.
- Modern symmetric-key ciphers algorithms rely on the use of product ciphers using alternating substitution and transposition phases.

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

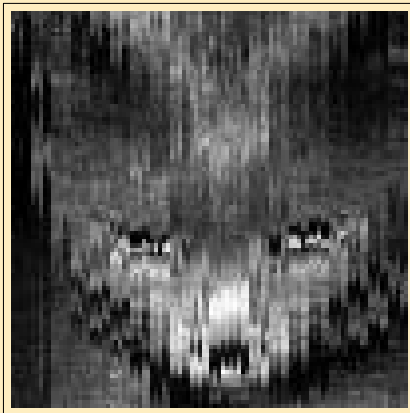
SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Small « arithmetic » of ciphers

Encryption with a permutation



Symmetric modern
Ciphers

Block cipher
modes of
operation

**Confusion and
Diffusion**

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Small « arithmetic » of ciphers

Encryption with a substitution (Ceasar)



Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

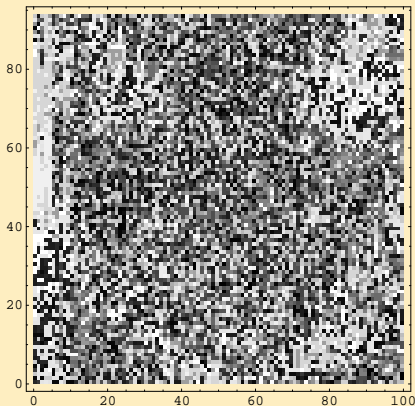
SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Small « arithmetic » of ciphers

Encryption with a permutation followed by a substitution



encryption

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

④ DES, 2DES & 3DES

DES : *Data Encryption Standard*

- LUCIFER (IBM/Feistel)
- The most famous symmetric-key algorithm (it's a block cipher)
- In 1973 : a contest by NBS (*without answer*)
- Another contest in 1974.
- In 1975 : IBM's proposition is known and published
- (Paranoia) : Answer (really) modified by NSA
- Adopted in 1977 as a Federal Information Processing Standards (FIPS)
- ANSI in 1981, refused as ISO

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

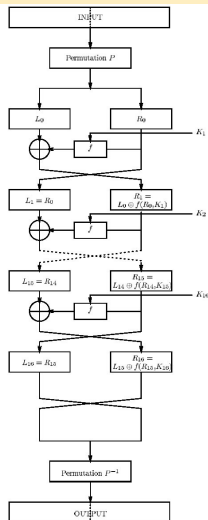
The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

DES : global view/1



DES : the archetypal block cipher (FIPS-74)

An algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstring of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is usually quoted as such.

Like other block ciphers, DES by itself is not a secure means of encryption but must instead be used in a mode of operation.

DES :

- It encrypts a message m of 64 bits, with a key k of 56 bits, into an encrypted message c of 64 bits
- Before the main rounds, the block is divided into two 32-bit halves and processed alternately ; this criss-crossing is known as the Feistel scheme :

$$m = L_0 || R_0$$

where

- L_0 : Leftmost 32 bits of the message
- R_0 Rightmost 32 bits of the message

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

DES :

- There are 16 identical stages of processing, termed rounds
- Each round is controlled by a subkey ($K_1, \dots K_{16}$)
- There is also an initial and final permutation, termed IP and FP, which are inverses (IP "undoes" the action of FP, and vice versa).
- IP and FP have almost no cryptographic significance, but were apparently included in order to facilitate loading blocks in and out of mid-1970s hardware, as well as to make DES run slower in software (to prevent brute-force attacks?).

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

DES : 16 very similar rounds/iterations

$$\left. \begin{aligned} L_0 \| R_0 &= P(m) \\ R_i &= L_{i-1} \oplus f(R_{i-1}, K_i) \\ L_i &= R_{i-1} \\ C_i &= L_i \| R_i \\ C &= P^{-1}(R_{16} \| L_{16}) \end{aligned} \right\} \text{ For } i = 1, \dots, 16 \quad (1)$$

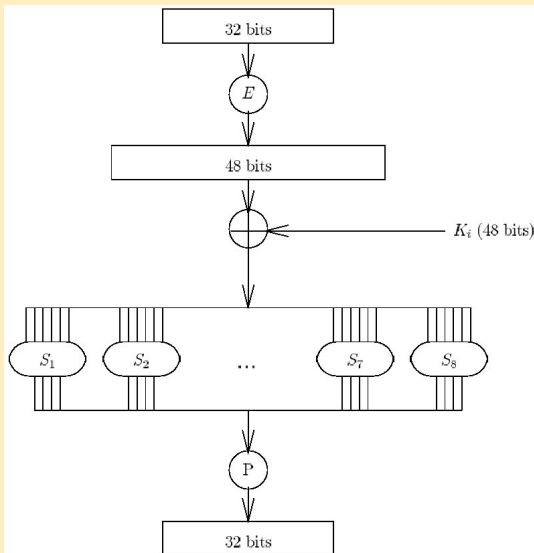
DES :

- L_i : the leftmost bits of c_i
- R_i : the rightmost bits of c_i

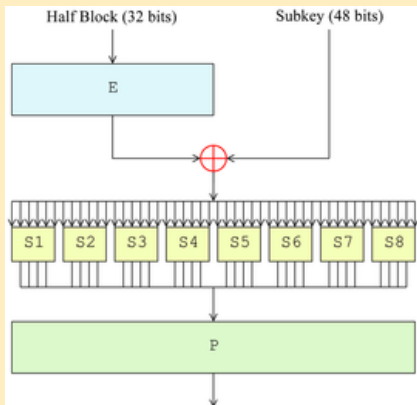
Some comments :

- ① The Round Function f is « complex » (see picture).
- ② How to decipher? very simple : same algorithm but you have to **reverse** the order of the 16 subkeys.

DES : Round Function



DES : Another view of the Round Function (*aka* Feistel (F) function)



Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

DES : Round Function

It is a function $f(R,K) : R$ with 32 bits and K with 48 bits

- 1 R is transformed in a 48 bits word with the expansion function E : 16 bits are unchanged, 16 are doubled
- 2 $E(R) \oplus K$ is separated in 8 strings, each of 6 bits :

$$B = B_1 \parallel B_2 \parallel B_3 \parallel B_4 \parallel \dots \parallel B_8$$

Each B_j is modified by the S-box S_j following :

- $B_j = (b_1, b_2, b_3, b_4, b_5, b_6)_2$, we compute the two integers
 - ① $I = (b_1, b_6)_2$
 - ② $J = (b_2, b_3, b_4, b_5)_2$
- $C_j = S_j(B_j) = S_j(I, J)$, where S_j is seen as a matrix (4,16) (so with 64 elements).

DES : The S-box S_1

There are 8 S-boxes, here is the first :

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

DES : some examples of the S-boxes S_1

000000	000001	101010	101011
14 = 1110	0 = 0000	6 = 0110	9 = 1001
111111	111110	011110	011111
13 = 1101	0 = 0000	7 = 0111	8 = 1000

The strict avalanche criterion (SAC) ...

is a formalization of the avalanche effect. It is satisfied if, whenever a single input bit is complemented, each of the output bits changes with a 50% probability. The SAC builds on the concepts of completeness and avalanche and was introduced by Webster and Tavares in 1985 [WIK].

DES : Expansion function E

- (1) With a word of R 32 bits, it gives a word $E(R)$ of 48 bits : expansion.
- (2) Some bits (16) of R are doubled : $16+32=48$.
- (3) See the following table (6)
- (4) Bits that are doubled : 32 and 1, 4 and 5, etc.
- (5) Bits that are not doubled : bits 2 and 3, 6 and 7, etc.

DES : Expansion Table

(6)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

DES : Examples with a round



Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

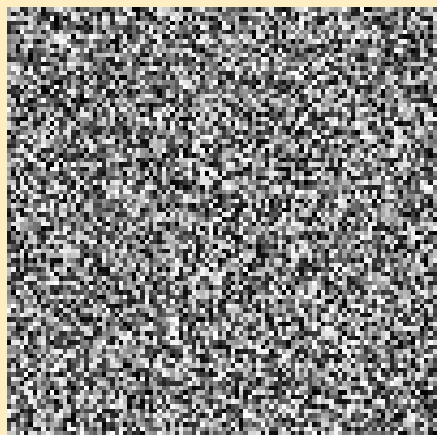
The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

DES : Examples with 8 rounds



Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

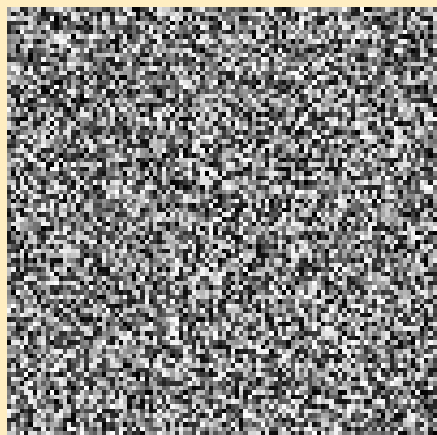
The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

DES : Examples with 16 rounds (complete)



Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

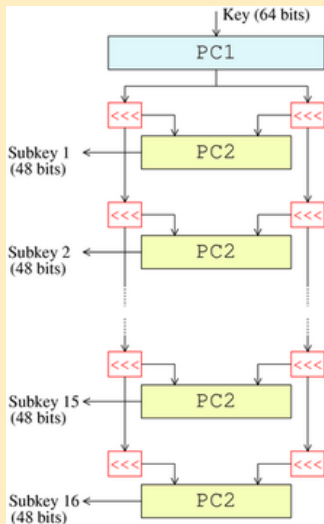
The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

DES : subkeys generation/Wikipedia



EPITA -
Cryptography

R. ERRA

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

DES : subkeys generation : PC1 with PC1_C and PC1_D

```
static char PC1_C[]=
{ 57,49,41,33,25,17, 9,
 1,58,50,42,34,26,18,
 10, 2,59,51,43,35,27,
 19,11, 3,60,52,44,36 };
```


DES : subkeys generation : PC1 with PC1_C and PC1_D

```
static char PC1_D[] =  
{ 63,55,47,39,31,23,15,  
  7,62,54,46,38,30,22,  
  14, 6,61,53,45,37,29,  
  21,13, 5,28,20,12, 4 };
```

Shift

```
/*Sequence of shifts for the key schedule. */  
static char shifts[] = { 1,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1, };
```

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

DES : cryptanalysis

- The main weakness : a key of 56 bits.
- EFF (*the Electronic Frontier Foundation* has published a book with the description of a 250 000 dollars computer, with asics.
- In 1991/1992 : the **linear cryptanalysis** and the **differential cryptanalysis** have been successful to break DES.
- But these attacks need a lot of couples (**clear text**, **encrypted text**).

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

nDES : 2DES & 3DES

- 3DES :
 - ① $3DES_{k_1,k_2,k_3}(m) = DES_{k_3}(DES_{k_2}^{-1}(DES_{k_1}(m)))$
 - ② 3DES : $3 \times 56 = 168$ bits
- 2DES :
 - ① $2DES_{k_1,k_2,k_1}(m) = DES_{k_1}(DES_{k_2}^{-1}(DES_{k_1}(m)))$
 - ② 2DES : $2 \times 56 = 112$ bits
- So $DES_{k_1}(m) = 3DES_{k_1,k_1,k_1}(m)$
- We can generalize $nDES$. Well you can do it (exercice).

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

**Other remarks
about DES**

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

⑤ Other remarks about DES

Weak and semi-weak keys of DES [Vau06]

- If $DES_k(DES_k)(m) = m$ we will say that k is a weak key. We know four weak keys : generated by $C = D = \{0\}^{28}$, $C = \{0\}^{28}$ and $D = \{1\}^{28}$, $C = \{1\}^{28}$ and $D = \{0\}^{28}$, $C = D = \{1\}^{28}$ with the key obtained using $PC1_{-1}(C|D)$ or with our notation $(PC1^{-1}_C|PC1^{-1}_D)$.
- If k is not weak and if there exists a key k' such that $DES_k^{-1} = DES_{k'}$. An example : $\{01\}^{14}|\{01\}^{14}|\{10\}^{10}|\{10\}^{14}$
- If \overline{m} is the bitwise complement of m then $DES_{\overline{k}}(\overline{m}) = \overline{DES_k(m)}$

Question (exercice) : can you define weak and semi-weak keys

- ① for 2DES?
- ② for 3DES?

Is DES a group?

- Let \mathcal{K} the set of all keys for DES : $\mathcal{K} \approx \{0^{56}, \dots 1^{56}\}$
- For two keys k_1 and k_2 we consider $DES_{k_1}(DES_{k_2}(m))$, we will write this $DES_{k_1 \circ k_2}$ and abusively we will talk about $k_1 \circ k_2$.

This stange question **Is DES a group?** means :
 $\forall k_1, k_2 \in \mathcal{K}$ does it exist a key k_3 such that

$$DES_{k_1}(DES_{k_2}(m)) = DES_{k_3}(m)?$$

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Is DES a group ?

- ① It seems it is not true. (Strongly supported by initial evidence and "proved" in 1993 by K. W. Campbell and M. J. Wiener at CRYPTO 92).
- ② If this would be true a consequence is 2DES and 3DES and nDES would be really **useless**.
- ③ But we don't know the answer to the following (interesting) question : is there a subset of \mathcal{K} such that (\mathcal{K}, \circ) is a group ?
- ④ If this subset exists : is it (very) small or (very) large ?

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

EPITA -
Cryptography

R. ERRA

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

⑥ AES/Rijndael

AES : Advanced Encryption Standard ([Sti10])

- AES has won in october 2000 the 2d AES Contest, organized by NIST
- It is the US Standard
- Approved by NSA (National Security Agency) in the *B1 suit*.
- AES= Rijndael : from the name of the two creators Joan Daemen et Vincent Rijmen.

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

The algorithm 1/2

- The (standard) algorithm takes as input a block of 128 bits
- The key can be of 128, 192 or 256 bits.
- There is an initial permutation of the 16 bytes=128 bits.
- These bytes are placed in a 4×4 matrix , lines are shifted.
- There is a linear transformation of the matrix done with a multiplication (see after) ...

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

The algorithm 2/2

- ... This multiplication is done in $GF(2^8)$ (a Field called the Galois Field).
- Last : a XOR between the matrix and another matrix gives an intermediate matrix.
- All these operations (repeated) define a round/iteration/tour
- The number **N**e of round varies :
 - ① 10 for a key of 128 bits
 - ② 12 for a key of 192 bits
 - ③ or 14 for a key of 256 bits.

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Algorithm 1 : AES

Input : (M, W) : M message, W expanded key (subkeys $\{K_0 \dots K_{Ne}\})$;

External Procedures : **SubBytes**, **ShiftRows** ;

MixColumns, **AddRoundKey** ;

Output : $AES(M, W)$

Begin :

$S = M$;

AddRoundKey(S, K_0) ;

For $i = 1$ **To** $Ne - 1$ **Do**

SubBytes(S) ; **ShiftRows**(S) ;

MixColumns(S) ; **AddRoundKey**(S, K_i) ;

EndFor ;

SubBytes(S) ; **ShiftRows**(S) ; **AddRoundKey**(S, K_i) ;

Return S

End.

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Description : Ne number of tours/rounds/iterations [Sti07]

- ① M : clear text.
- ② $S=M$ (**State**).
- ③ **RoundKey** is XORed with **State**
- ④ For each of the (Ne-1) rounds with the **S** box we execute **SubBytes** on **State**.
- ⑤ We do a permutation **ShiftRows** on **State**
- ⑥ Followed by a permutation **MixColumns** on **State**
- ⑦ Last : we add **AddRoundKey**
- ⑧ Last round : **SubBytes** followed by **ShiftRows** and we finish by **AddRoudKey**.
- ⑨ No **MixColumns** for the last round.
- ⑩ The Ciphersed Text C is defined as the last value of the **State S**.

M : message of 128 bits = 16 bytes($M_{0,0} \dots M_{3,3}$),

State =

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

←

$M_{0,0}$	$M_{0,1}$	$M_{0,2}$	$M_{0,3}$
$M_{1,0}$	$M_{1,1}$	$M_{1,2}$	$M_{1,3}$
$M_{2,0}$	$M_{2,1}$	$M_{2,2}$	$M_{2,3}$
$M_{3,0}$	$M_{3,1}$	$M_{3,2}$	$M_{3,3}$

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

ShiftRows Operations on S=State

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$	←	$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$		$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	$s_{1,0}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$		$s_{2,2}$	$s_{2,3}$	$s_{2,0}$	$s_{2,1}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$		$s_{3,3}$	$s_{3,0}$	$s_{3,1}$	$s_{3,2}$
					<< 0			
					<< 1			
					<< 2			
					<< 3			

SubBytes($a_7a_6a_5a_4a_3a_2a_1a_0$) (Algo 2)

- **SubBytes** executes a substitution on each byte of **State**
- **SubBytes** uses the S box (unique in AES) π_S : a permutation of $\{0, 1\}^8$
- S is a matrix 16×16 : $S(X, Y)$ obtained via $(X|Y)_{16}$ (hexadecimal on a byte)
- The action of S can also be represented from an algebraic point of view.

S-box of AES

	Y															R. ERKA	
X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0	63	7C	77	7B	F2	6B	...								Symmetric modern Cipher	76	
1	CA						...								Block cipher		
2	B7						...								modes of operation		
3	04						...										
4	09						...								Confusion and Diffusion		
5	53	D1	00	ED			...										
6	D0						...								DES, 2DES & 3DES		
7	51						...								Other remarks about DES		
8	CD						...										
9	60						...								AES/Rijndael		
A	E0						...										
B	E7						...								Cryptographic Hash Functions		
C	BA						...										
D	70						...								The Hash Function MD4 (simplified)		
E	E1						...								SHA-1 (short version)		
F	8C	A1	77	7B	F2	6B	...									16	

Summary of modern

Ciphers

Block cipher

modes of

operation

Confusion and

Diffusion

DES, 2DES & 3DES

Other remarks

about DES

AES/Rijndael

Cryptographic

Hash Functions

The Hash Function

MD4 (simplified)

SHA-1 (short

version)

Hash functions :

Uses

Attacks of SHA-0

Algorithm 2 : SubBytes($a_7a_6a_5a_4a_3a_2a_1a_0$)

Input : $a_7a_6a_5a_4a_3a_2a_1a_0$;

External Procedures : FieldInv, BinaryToField, FieldToBinary ;

Output : ($b_7b_6b_5b_4b_3b_2b_1b_0$)

Begin :

$z \leftarrow \text{BinaryToField}(a_7a_6a_5a_4a_3a_2a_1a_0)$

If $z \neq 0$ **Then** $z \leftarrow \text{FieldInv}(z)$

$(a_7a_6a_5a_4a_3a_2a_1a_0) \leftarrow \text{FieldToBinary}(z)$

$(c_7c_6c_5c_4c_3c_2c_1c_0) \leftarrow (01100011)$

For $i = 0$ **To** 7

$b_i \leftarrow (a_i + a_{i+4} + a_{i+5} + a_{i+6} + a_{i+7} + c_i) \bmod 2$

Return ($b_7b_6b_5b_4b_3b_2b_1b_0$)

Fin.

Symmetric modern
CiphersBlock cipher
modes of
operationConfusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash FunctionsThe Hash Function
MD4 (simplified)SHA-1 (short
version)Hash functions :
Uses

Attacks of SHA-0

MixColumns(c) (Algo 3)

- **MixColumns** : executed on each of the 4 columns of **State** (c)
- So, each column is replaced by a new column
- The multiplication Matrix x Vector is done in the Galois Field \mathbb{F}_{2^8}
- The addition is done in the field modulo 2 (i.e. exclusive OR \oplus).

Algorithm 3 : MixColumns

Input : $c_7c_6c_5c_4c_3c_2c_1c_0$;

External Procedures : FieldMult, BinaryToField, FieldToBinary ;

Output : $(b_7b_6b_5b_4b_3b_2b_1b_0)$

Begin :

For $i = 0$ **To** 3 $t_i \leftarrow \text{BinaryToField}(s_{i,c})$

$u_0 \leftarrow \text{FieldMult}(x, t_0) \oplus \text{FieldMult}(x + 1, t_0) \oplus t_2 \oplus t_3$

$u_1 \leftarrow \text{FieldMult}(x, t_1) \oplus \text{FieldMult}(x + 1, t_1) \oplus t_3 \oplus t_0$

$u_2 \leftarrow \text{FieldMult}(x, t_2) \oplus \text{FieldMult}(x + 1, t_2) \oplus t_0 \oplus t_1$

$u_3 \leftarrow \text{FieldMult}(x, t_3) \oplus \text{FieldMult}(x + 1, t_3) \oplus t_1 \oplus t_2$

For $i = 0$ **To** 3 $s_{i,c} \leftarrow \text{FieldToBinary}(u_i)$

End.

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Algebraic Version of S

- π_S uses operations in the Galois Finite Field $\mathbb{F}_{2^8} = \mathbb{Z}_2[x](p(x) = x^8 + x^4 + x^3 + x^2 + x + 1)$.
- Example : $(53)_{16} = (01010011)_2 = (0101|0011)_2$
- In $\mathbb{F}_{2^8} = \mathbb{Z}_2[x](x^8 + x^4 + x^3 + x^2 + x + 1)$:
 $(53)_{16} = x^6 + x^4 + x + 1$
- The inverse of this polynomial in \mathbb{F}_{2^8} is :
 $x^7 + x^6 + x^3 + x$
- *i.e.* : $(x^7 + x^6 + x^3 + x) * (x^6 + x^4 + x + 1) = 1 \bmod p(x)$
- $(a_7a_6a_5a_4a_3a_2a_1a_0) = (11001010)$
- $b_0 = a_1 + a_5 + a_6 + a_7 \bmod 2 = 1$ etc.
- $(b_7b_6b_5b_4b_3b_2b_1b_0) = (11101101) = (ED)_{16}$
- So $S(5_{16}, 3_{16}) = (ED)_{16}$ (See the Table of the S-Box).

KeyExpansion(key) (Algo 4)

- **KeyExpansion**(key)
- AES : 10 rounds for a key of 128 bits
- So we need 11 subkeys of 16 bytes =128 bits
- With a word of 32 bits each subkey needs 4 words.
- Concatenation of the subkeys : (*Expanded Key*).
- $(w_0w_1 \cdots w_{43})$: w_i is a 32 bits word.

KeyExpansion(key) (Algo 4)

- key : 128 bits decomposed as 16 bytes :
($\{key(0), \dots, key(15)\}$)
- **RotWord**(B_0, B_1, B_2, B_3) : a rotation of the four bytes
gives B_1, B_2, B_3, B_0
- **SubWord**(B_0, B_1, B_2, B_3) : we apply the S box on
each of the bytes : gives B'_0, B'_1, B'_2, B'_3 with
- $B'_i = \text{SubBytes}(B_i)$
- RCon : constants.

Algorithm 4 : KeyExpansion

Input : Key ;

External Procedures : RotWord, SubWord ;

Output : ($W_0 W_1 \dots W_{43}$)

Begin :

$RCon[1] \leftarrow 01000000$; $RCon[2] \leftarrow 02000000$; $RCon[3] \leftarrow 04000000$;

$RCon[4] \leftarrow 08000000$; $RCon[5] \leftarrow 10000000$;

$RCon[6] \leftarrow 20000000$; $RCon[7] \leftarrow 40000000$; $RCon[8] \leftarrow 80000000$;

$RCon[9] \leftarrow 1B000000$; $RCon[10] \leftarrow 36000000$;

For $i = 0$ **To** 3 **Do** $w_i \leftarrow (key[4i], key[4i + 1], key[4i + 2], key[4i + 3])$;

For $i = 4$ **To** 43 **Do**

temp $\leftarrow w[i-1]$

If $i \equiv 0 \bmod 4$ **Then** temp $\leftarrow \text{SubWord}(\text{RotWord}(\text{temp})) \oplus RCon[i/4]$

$w[i] \leftarrow w[i-4] \oplus \text{temp}$

Return (w_0, w_1, \dots, w_{43})

Comment : we need 11 subkeys of subkeys, each with 4 words of 32 bits

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

**Cryptographic
Hash Functions**

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

7 Cryptographic Hash Functions

We can send

- The message (possibly enciphered)
- The signature

But this means :

- we double the length of the "message"
- we double the time needed.

So, we use a *cryptographic hash functions*.

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

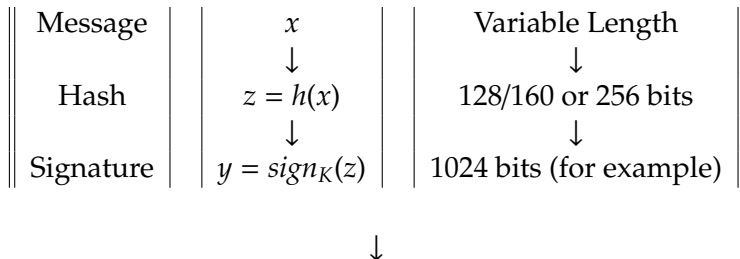
Hash functions :
Uses

Attacks of SHA-0

- ① Variable Size Input
- ② Fixed output size
- ③ Efficient computation
- ④ Pseudorandom
- ⑤ *Pre-image Resistant* : one-way
It is not possible to find x , given $H(x)$.
- ⑥ *2nd Pre-image Resistant* : *Weak Collision Resistant*
It is computationally difficult to find y , such that
 $H(y) = H(x)$
- ⑦ *Strong Collision Resistant* :
It is computationally difficult to find any two x and y ,
such that $H(y) = H(x)$.

Cryptographic hash function : to sign a long message

Symmetric cryptography faster than **Asymmetric cryptography** : we sign the hash !



Message, hash (fingerprint), signature : numerical !

Examples of Crypto Hash Functions

- ① MD4 = Message Digest 4 [RFC 1320] : 32-bit
- ② MD5 = Message Digest 5 [RFC 1321] : 32-bit
- ③ SHA0 = ex SHA, Secure hash algorithm [NIST]
- ④ SHA-1 = Updated SHA
- ⑤ SHA-2 = SHA-224, SHA-256, SHA-384, SHA-512
- ⑥ SHA-512 uses 64-bit
- ⑦ SHA-3 : the future

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

**The Hash Function
MD4 (simplified)**

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

8 The Hash Function MD4 (simplified)

- ① x : message
- ② $m = x || 1 || 0 \cdots 0 || l$
 - ① with $Length(m) = 448$ [modulo 512] and
 - ② $l := Length(x)$ on 64 bits $448 + 64 = 512$
- ③ $M = m[0]m[1] \cdots m[N - 1]$
- ④ $N = 0$ [modulo 16]
- ⑤ $A = 67452301$ (Hex)
- ⑥ $B = efcdab89$
- ⑦ $C = 98badcfe$
- ⑧ $D = 10325476$

- **For** $i = 0$ To $N/16 - 1$ **Do**
- **For** $j = 0$ To 15 **Do**
 - ① $X[j] = M[16i + j]$
 - ② $AA = A;$
 - ③ $BB = B$
 - ④ $CC = D;$
 - ⑤ $DD = D$
 - ⑥ **Step 1 + Step 2 + Step 3 (similar)**
- **EndFor**
- **EndFor**

Step 1

- $A = (A + f_1(B, C, D) + X[0]) \lll 3$
- $D = (D + f_1(A, B, C) + X[1]) \lll 7$
- $C = (C + f_1(D, A, B) + X[2]) \lll 11$
- $B = (B + f_1(C, D, A) + X[3]) \lll 19$
- ...
- $B = (B + f_1(C, D, A) + X[15]) \lll 19$

With

$$f_1(X, Y, Z) = (X \text{ AND } Y) \text{ OR } ((\text{NOT } X) \text{ AND } Z)$$

Step 1, 2 & 3

- $f_1(X, Y, Z) = (X \text{ AND } Y) \text{ OR } ((\text{NOT } X) \text{ AND } Z)$
- $f_2(X, Y, Z) = (X \text{ AND } Y) \text{ OR } (X \text{ AND } Z) \text{ OR } (Y \text{ AND } Z)$
- $f_3(X, Y, Z) = X \text{ XOR } Y \text{ XOR } Z$

Step 2 : $C_2 = 5A827999$

- $A = (A + f_2(B, C, D) + X[0]) + C_2 \ll 3$
- $D = (D + f_2(A, B, C) + X[4]) + C_2 \ll 5$
- $C = (C + f_2(D, A, B) + X[8]) + C_2 \ll 9$
- $B = (B + f_2(C, D, A) + X[12]) + C_2 \ll 13$
- $A = (A + f_2(B, C, D) + X[1]) + C_2 \ll 3$
- $D = (D + f_2(A, B, C) + X[5]) + C_2 \ll 5$
- $C = (C + f_2(D, A, B) + X[9]) + C_2 \ll 9$
- $B = (B + f_2(C, D, A) + X[13]) + C_2 \ll 13$
- ...
- $B = (B + f_2(C, D, A) + X[15]) + C_2 \ll 13$

Step 3 : $C_3 = 6ED9EBA1$

- $A = (A + f_3(B, C, D) + X[0]) + C_3 \ll 3$
- $D = (D + f_3(A, B, C) + X[8]) + C_3 \ll 9$
- $C = (C + f_3(D, A, B) + X[4]) + C_3 \ll 11$
- $B = (B + f_3(C, D, A) + X[12]) + C_3 \ll 15$
- $A = (A + f_3(B, C, D) + X[2]) + C_3 \ll 3$
- $D = (D + f_3(A, B, C) + X[6]) + C_3 \ll 9$
- $C = (C + f_3(D, A, B) + X[10]) + C_3 \ll 11$
- $B = (B + f_3(C, D, A) + X[14]) + C_3 \ll 15$
- ...
- $B = (B + f_3(C, D, A) + X[15]) + C_3 \ll 15$

MD4 hash :

Then perform the following additions. (That is, increment each of the four registers by the value it had before this block was started.)

- $A = A + AA$ (modulo 2^{32} : implicit)
- $B = B + BB$
- $C = C + CC$
- $D = D + DD$

and : actually $MD4(m) = A|B|C|D$.

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

**SHA-1 (short
version)**

Hash functions :
Uses

Attacks of SHA-0

9 SHA-1 (short version)

SHA-1(m) :

$(A, B, C, D, E) \leftarrow$ Initial values
(5 registers of 32 bits)

$m || 10 \dots 0 || \ell = M_0 || \dots || M_{N-1}$
(N blocks of 512 bits)

For $n=0, \dots, N-1$ Do

$M_n \rightarrow X_0 || \dots || X_{79}$

(Expansion in 80 blocks of 32 bits)

For $i=0, \dots, 79$ Do

$(A, B, C, D, E) \leftarrow f_i(A, B, C, D, E, X_i)$

Return (A, B, C, D, E)

EPITA -
Cryptography

R. ERRA

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

**Hash functions :
Uses**

Attacks of SHA-0

⑩ Hash functions : Uses

- Hash functions are used to get a digest of a message
Must take variable size input, produce fixed size pseudorandom output, be efficient to compute
- Cryptographic hash functions should be preimage resistant, 2nd preimage resistant, and collision resistant (*i.e. reminder : computationally difficult*)
- Cryptographic hashes are used for **message authentication, digital signatures, password storage**
- SHA-1 produces 160 bit output, SHA-224, SHA-256, SHA-384, and SHA-512 produce 224, 256, 384, and 512 bit outputs. All consist of 80 rounds.

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

11 Attacks of SHA-0

12 August 2004 : a collision on SHA-0

By analyzing the differences between *SHA-0* and *SHA-1* Antoine Joux (and his team) have found a true collision on *SHA-0* :

```
a766a602 b65cffe7 73bcf258 26b322b3 d01b1a97 2684ef53 3e3b4b7f 53fe3762
24c08e47 e959b2bc 3b519880 b9286568 247d110f 70f5c5e2 b4590ca3 f55f52fe
effd4c8f e68de835 329e603c c51e7f02 545410d1 671d108d f5a4000d cf20a439
4949d72c d14fbb03 45cf3a29 5dcda89f 998f8755 2c9a58b1 bdc38483 5e477185
f96e68be bb0025d2 d2b69edf 21724198 f688b41d eb9b4913 fbe696b5 457ab399
21e1d759 1f89de84 57e8613c 6c9e3b24 2879d4d8 783b2d9c a9935ea5 26a729c0
6edfc501 37e69330 be976012 cc5dfe1c 14c4c68b d1db3ecb 24438a59 a09b5db4
35563e0d 8bdf572f 77b53065 cef31f32 dc9dbaa0 4146261e 9994bd5c d0758e3d
```

```
a766a602 b65cffe7 73bcf258 26b322b1 d01b1ad7 2684ef51 3e3b4b7f d3fe3762
a4c08e45 e959b2fc 3b519880 39286528 a47d110d 70f5c5e0 34590ce3 755f52fc
6ffd4c8d 668de875 329e603e 451e7f02 d45410d1 e71d108d f5a4000d cf20a439
4949d72c d14fbb01 45cf3a69 5dcda89d 198f8755 ac9a58b1 3dc38481 5e4771c5
796e68fe bb0025d0 52b69edd a17241d8 7688b41f 6b9b4911 7be696f5 c57ab399
a1e1d719 9f89de86 57e8613c ec9e3b26 a879d498 783b2d9e 29935ea7 a6a72980
6edfc503 37e69330 3e976010 4c5dfe5c 14c4c689 51db3ecb a4438a59 209b5db4
35563e0d 8bdf572f 77b53065 cef31f30 dc9dbae0 4146261c 1994bd5c 50758e3d
```

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

12 The future : SHA-3?

The future : SHA-3?

SHA-3? see [NIS] on Documentation Center

The National Institute of Standards and Technology (NIST) is in the process of selecting a new cryptographic hash algorithm through a public competition. The new hash algorithm will be referred to as 'SHA-3' and will complement the SHA-2 hash algorithms currently specified in Federal Information Processing Standard (FIPS) 180-3, Secure Hash Standard [1]. The selected algorithm is intended to be suitable for use by the U.S. government, as well as the private sector and, at the completion of the competition, to be available royalty-free worldwide. The competition will be referred to as the SHA-3 competition hereafter in this document. The competition is NIST's response to recent advances in the cryptanalysis of hash algorithms, including the government standard SHA-1 hash algorithm [1, 2].

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

The future : SHA-3 ?

SHA-3 see [NIS]

An attack by Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu [3], and extended by many others, has seriously called into question the security of SHA-1's use in digital signatures and other applications that require collision resistance. While the SHA-2 family [1] of hash algorithms provides an immediate alternative, NIST expects the selected SHA-3 to offer security that is at least as good as the SHA-2 algorithms with significantly improved efficiency or additional features. In preparation for the SHA-3 competition, NIST held workshops on October 31-November 1, 2005 [4] and August 24-25, 2006 [5] to discuss the status of hash algorithms and develop a path forward for developing a new hash algorithm standard. As a result, NIST instituted a public competition, similar to that used to select the Advanced Encryption Standard (AES) [6, 7]. [...]

SHA-3 see [NIS]

- NIST received 64 candidate algorithm by the October 31, 2008 entry deadline for the SHA-3 competition.
- Of these, NIST accepted 51 first-round candidates as meeting the minimum acceptance criteria for being 'complete and proper submissions', as defined in FRN-Nov07. These criteria included provisions for reference and optimized C code implementations, known-answer tests, a written specification, and required intellectual property statements.
- In addition, the algorithms were required to be implementable in a wide range of hardware and software platforms, support message digest sizes of 224, 256, 384, 512 bits, and support a maximum message length of at least 2^{64} bits.
- NIST selected 51 entries for the Round 1 and 14 of them advanced to Round 2.

EPITA -
Cryptography

R. ERRA

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

The future : SHA-3 ?

Proposal for SHA-3 see [WIK, NIS] :Accepted for Round Two

The following hash function submissions have been accepted for Round Two :

- BLAKE
- Blue Midnight Wish
- CubeHash (Bernstein)
- ECHO (France Telecom)
- Fugue (IBM)
- Grøstl (Knudsen et al.)
- Hamsi
- JH
- Keccak (Keccak team, Daemen et al.)
- Luffa
- Shabal
- SHAvite-3
- SIMD
- Skein (Schneier et al.)

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Proposal for SHA-3 see [WIK, NIS] : : Conceded entrants

The following Round One entrants have been officially retracted from the competition by their submitters ; they are considered broken according to the NIST official Round One Candidates web site. As such, they are withdrawn from the competition.

- Abacus
- Boole
- DCH
- Khichidi-1
- MeshHash
- SHAMATA
- StreamHash
- Tangle
- WaMM
- Waterfall

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Proposal for SHA-3 see [WIK, NIS] : Rejected entrants

Several submissions received by NIST were not accepted as First Round Candidates, following an internal review by NIST. In general, NIST gave no details as to why each was rejected. NIST also has not given a comprehensive list of rejected algorithms; there are known to be 13, **but only the following are public.**

- HASH 2X
- Maraca
- NKS 2D
- Ponic
- ZK-Crypt

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)

SHA-1 (short
version)

Hash functions :
Uses

Attacks of SHA-0

Proposal for SHA-3 see [WIK, NIS] : The winner is
Keccak (Keccak team, Daemen et al.)

- SHA3 : a subset of the cryptographic primitive family Keccak
- Designed by Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche,
- Building upon RadioGatun.
- SHA-3 is a member of the Secure Hash Algorithm family.
- The SHA-3 standard was released by NIST on August 5, 2015.

Symmetric modern
Ciphers

Block cipher
modes of
operation

Confusion and
Diffusion

DES, 2DES & 3DES

Other remarks
about DES

AES/Rijndael

Cryptographic
Hash Functions

The Hash Function
MD4 (simplified)


SHA-1 (short
version)


Hash functions :
Uses


Attacks of SHA-0

 A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone.
Handbook of Applied Cryptography.
CRC Press, 1997.

<http://cacr.uwaterloo.ca/hac/> (all chapters available
for free download).

 NIST.
Cryptographic hash – THE SHA-3 PROJECT.
<http://csrc.nist.gov/groups/ST/hash/>.

 D. Stinson.
Cryptographie, Théorie et Pratique (2ème édition).
Vuibert, 2007.

 D. Stinson.
Cryptography.
2010.

 S. Vaudenay.

Introduction to classical cryptography.
Springer, 2006.



WIKIPEDIA.

[http ://www.wikipedia.org](http://www.wikipedia.org).