

Introduction to Modern Cryptography

Benny Chor

More Block Ciphers: DES and AES

Lecture 3 Part II

Tel-Aviv University

revised Feb. 5th, 2008

Block Ciphers: Design Principles

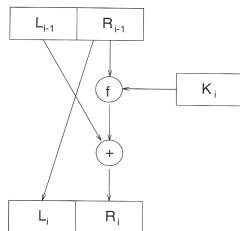
Fairly simple building blocks, each implementing a **keyed permutation**. These building blocks are iterated, possibly with different parts of key, to generate a (hopefully) strong cipher, featuring

- Bit-shuffling (often called permutation boxes). Creates so called **confusion** – making the relationship between the key and the ciphertext as complex and involved as possible (Shannon, 1949).
- Simple non-linear functions (often called substitution boxes). Creates so called **diffusion** – redundancy in the statistics of the plaintext should be "dissipated" in the statistics of the ciphertext.
- **Key mixing**: Linear (mod 2) mixing, by XORing "key schedule" at beginning of each iteration.

Properties:

- High speed.
- Fixed block size (typically 64, 128, 256 bits).
- Ciphertext is a non-linear function of key and message bits.

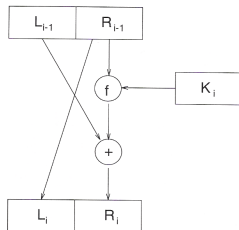
Feistel Networks



Encryption (and decryption) is done by identical iterations, or **rounds**. Here we consider the i -th round.

- The input to this round consists of the previous output, $P = L_{i-1}|R_{i-1}$, where L_{i-1}, R_{i-1} are of the same length.
- $R_i = L_{i-1}$ (shifted, unchanged, to the right side of the output).
- $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$, where K_i is the key (portion) for round i .
- f should be a keyed function that is at least **mildly hard** to invert. It **need not** be a permutation.
- How is **decryption** done?

Feistel Networks - Properties



- No matter which function is used as f , we obtain a permutation (namely F is reversible even if f is not).
- The same code/circuit, with keys deployed in reverse order, can be used for decryption.
- **Important Theoretical Result:** If f is a pseudo-random function then **four rounds** of Feistel network yield a pseudo-random **permutation** (Luby and Rackoff, 1988).

DES – Historic Note

The DES (data encryption standard) is a symmetric (private key) block cipher, using 64 bit blocks and a **56 bit key**. Has 16 round **Feistel network**, where each round key is a 48 bit subset of the complete key.

Developed at IBM, it was approved by the US government (in **1976**) as a standard. Size of key (**56 bit**) was apparently small enough to allow the mighty NSA (US national security agency) to break it exhaustively even back in 70s.

Throughput is 10Mb/sec in software, and 1Gb/sec in hardware (back in 1991!).

Criticized for unpublished design decisions (designers did not want to disclose **differential cryptanalysis**, which they discovered).

In the 90s it became clear that DES is too weak for contemporary hardware & algorithmics. (Best attack, Matsui **linear attack**, requires only $\approx 2^{41}$ known plaintext/ciphertext pairs.)

Historic Note (cont.)

The US government NIST (national inst. of standards and technology) announced a call for an advanced encryption standard in 1997.

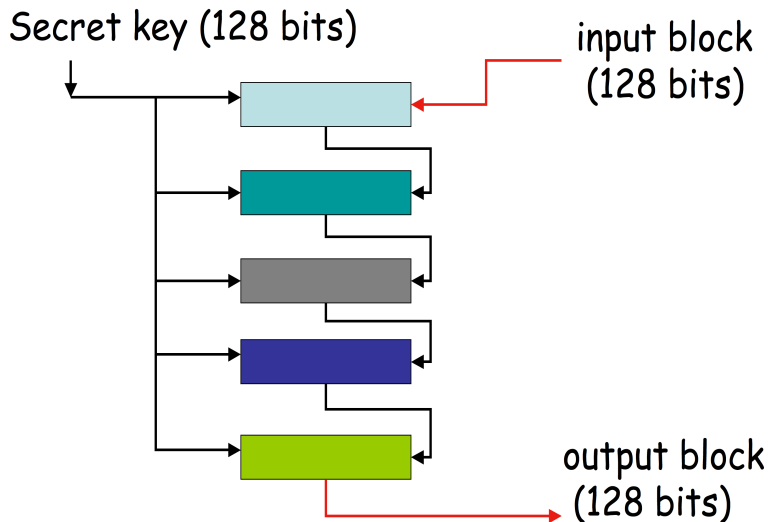
This was an international open competition. Overall, nine proposals were made and evaluated, and five were finalists. Out of those, a proposal named **Rijndael**, by Daemen and Rijmen (two Belgians) was chosen in February 2001.

AES - Advanced Encryption Standard

- Symmetric block cipher.
- Key lengths: 128, 192, or 256 bits.
- Approved US standard (2001).

- Resistant to all **known** attacks.
- Very fast.
- Compact code.
- Simple (kind of).

AES Encryption/Decryption: Carried out in Ten Rounds



AES Specifications: State

- Input & output **block length**: 128 bits.
- **State**: 128 bits, arranged in a 4-by-4 matrix of bytes.
- Each byte is viewed as an element in $GF(2^8)$.

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

Rounds in AES

128 bits AES uses 10 rounds. These are **not** Feistel rounds.

- The **secret key** is expanded from 128 bits to 10 **round keys**, 128 bits each.
- Each round changes the state, then XORS the round key.

Each rounds complicates things a little. Overall it seems **infeasible** to invert without the secret key (but easy given the key).

AES Specifications: One Round

Transform the **state** by applying:

1. Substitution.
2. Shift rows.
3. Mix columns.
4. XOR **round key**

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

1) **Substitution** operates on every byte separately: $S_{i,j} \leftarrow S_{i,j}^{-1}$
(multiplicative inverse in $GF(2^8)$, which is highly **non-linear**).
If $S_{i,j} = 0$, don't change it.

Clearly, the substitution is invertible.

Cyclic Shift of Rows

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$	(no shift)
$S_{1,3}$	$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	(shift one position)
$S_{2,2}$	$S_{2,3}$	$S_{2,0}$	$S_{2,1}$	(shift two positions)
$S_{3,1}$	$S_{3,2}$	$S_{3,3}$	$S_{3,0}$	(shift three positions)

Clearly, the shift is **invertible**.

Mix Columns

MixCol maps the state to a new one.

It multiplies each column of state by the polynomial $c(x)$ mod $x^4 + 1$, where $c(x) = 0x03 \cdot x^3 + 0x01 \cdot x^2 + 0x01 \cdot x + 0x02$.

More precisely, for the first column,

$$S'_{0,0} \cdot x^3 + S'_{1,0} \cdot x^2 + S'_{2,0}x + S'_{3,0} = (0x03 \cdot x^3 + 0x01 \cdot x^2 + 0x01 \cdot x + 0x02) \cdot (S_{0,0}x^3 + S_{1,0} \cdot x^2 + S_{2,0} \cdot x + S_{3,0}) \text{ mod } x^4 + 1.$$

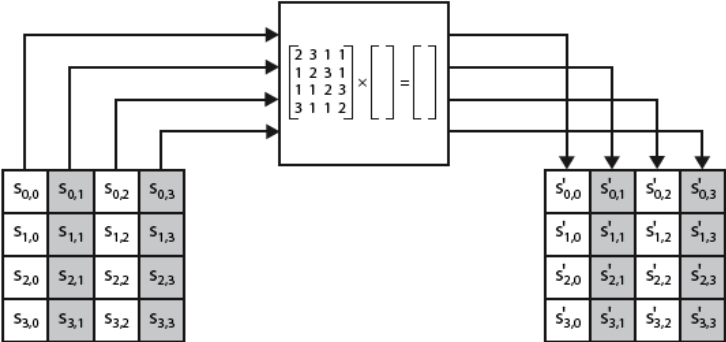
The inverse operation is **InvMixCol**: It multiplies each column of state by the polynomial $d(x)$ mod $x^4 + 1$, where

$$d(x) = 0x0b \cdot x^3 + 0x0d \cdot x^2 + 0x09 \cdot x + 0x0e.$$

Comment: All these coefficients from $c(x)$ and $d(x)$ (**0x03**, **0x01**, **0x02**, **0x0b**, **0x0d**, **0x09**, **0x0e**) are simply constants from $GF(2^8)$ (or bytes, if this makes you feel better :-).

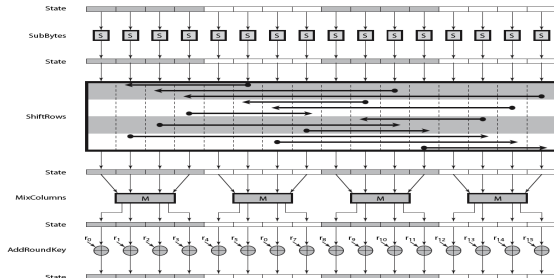
Comment 2: These $c(x)$ and $d(x)$ correspond to the first (left most) column. The other columns have different but similar coefficients/polynomials.

Mix Columns, the Movie



(taken from a presentation by William Stallings, drawing by Lawrie Brown)

AES, Famous Last Words



- Expanding key to round keys, and xoring with the state, are not too complicated either, but are **not discussed here**.
- See the original document at www.daimi.au.dk/~ivan/rijndael.pdf, for further details.
- Attacks against 2 rounds AES are known.
- But for full, 10 round AES, this is considered infeasible and breaking AES **efficiently** an **open problem**.