5.2.4. Design Considerations & Security

- After 2 rounds full diffusion holds, i.e., if one byte is changed in the input all bytes are changed after rounds.
- S-box is constructed as $x \mapsto x^{-1}$ in $\mathbb{F}_{2^8}$.
  Advantages:
  - simple, algebraic, highly nonlinear
  - Resisting differential and linear cryptanalysis
  - No suspicion of trapdoor built in. (other than DES)
- ShiftRows to resist two recent attacks: truncated differentials and square attack.
- MixColumns causes diffusion among bytes.
- Key Schedule to avoid advantages from knowing parts of the key.
- Presently no better attacks than exhaustive search are known against AES 128.
  Attacks against AES 192 and AES 256 of complexity $\sim 2^{119}$. Not working against AES 128. Hence, AES 128 is better than the others.
  (see www.schneier.com/blog/....)

5.3. Other Block Ciphers

- IDEA (International Data Encryption Algorithm) (Lai & Massey, 1990, Ascom, Switzerland)
- RC5 (Ronald Rivest, 1994)
- Blowfish (B. Schneier, 1993)
- Serpent (Anderson, Biham, Knudsen, 1998)

5.4. Modes of Operation

Let BC_K be a block cipher on blocks of fixed length using key K. 5 modes of operation were standardized in Dec. 1980.

5.4.1. ECB (electronic codebook mode)

Direct use BC_K. Plaintext blocks $M_1, M_2, M_3, \dots$

Encryption $\quad C_i = BC_K(M_i)$, $i = 1, 2, \dots$

Decryption $\quad M_i = BC_K^{-1}(C_i)$, $i = 1, 2, \dots$

5.4.2. CBC (cipher blockchaining mode)

Given: Plaintext blocks $M_1, M_2, \ldots$
key K
Initial vector (IV) C_0 (non secret) } (*)

Encryption: $C_i = BC_K(C_{i-1} \oplus M_i)$, $i = 1, 2, \ldots$

Decryption: $C_{i-1} \oplus M_i = BC_K^{-1}(C_i)$, hence
$M_i = BC_K^{-1}(C_i) \oplus C_{i-1}$, $i = 1, 2, \ldots$

5.4.3. OFB (output feedback mode)

Given (*), $z_0 = C_0$

Encryption: $z_i = BC_K(z_{i-1})$, $C_i = M_i \oplus z_i$

Decryption: " , $M_i = C_i \oplus z_i$, $i = 1, 2, \ldots$

A key stream $z_1, z_2, \ldots$ is generated and x-ored with the message, see one-time pad.

5.4.4. CFB (cipher feedback mode)

Given (*)

Encryption: $z_i = BC_K(C_{i-1})$, $C_i = M_i \oplus z_i$

Decryption: $M_i = C_i \oplus z_i = C_i \oplus BC_K(C_{i-1})$, $i = 1, 2, \ldots$

The key stream ~~is base~~ depends on the predessor cipher block.

Thinking the Future
Zukunft denken

5.4.5. CTR (counter mode)

Given (*), $Z_0 = C_0$ (interpreted as some integer)

Encryption: $Z_i = Z_{i-1} + 1$, $C_i = BC_K(Z_i) \oplus M_i$

Decryption: " , $M_i = BC_K(Z_i) \oplus C_i$, $i = 1, 2, \ldots$

Applications:

Example: MAC (message authentication code)

In CBC and CFB modes, changing any bit in the message affects all subsequent blocks.

Generate a MAC.

- Append C_n to the message $(M_1, \ldots, M_n)$
  If O/E tempers with the message, C_n does not fit any more.
- The authorized receiver, knowing K, can easily verify C_n, hence, verify the integrity or authenticity of $(M_1, \ldots, M_n)$

<u>Example.</u> Storing passwords

- User types (name, password)
- System generates a key $K = K(\text{name}, \text{passwd})$ and stores $(\text{name}, BC_K(\text{passwd}))$
- When logging in, system compares ~~(name, passwd~~ $(\text{name}, BC_K(\text{passwd}))$ with the stored value.

Knowledge of $(\text{name}, BC_K(\text{passwd}))$ is useless for an intruder.

6. Number-Theoretic Reference Problems

Consider $\mathbb{Z}_n$: ring of equivalence classe modulo n

$s, t \in \mathbb{Z}$, $s \sim t$ or $s \equiv t \pmod{n} \Leftrightarrow n \mid (s-t)$

($\sim$ equivalence relation on $\mathbb{Z}$)

$(\mathbb{Z}_n, +, \cdot)$ forms a ring: $(\mathbb{Z}_n, +)$ Abelian group, $(\mathbb{Z}_n, \cdot)$ associativ, 1 exists & distr. laws.

<u>Def. 6.1.</u> $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a,n) = 1\}$

is called the <u>multiplicative group</u> of $\mathbb{Z}_n$.

$\varphi(n) = \underbrace{|\mathbb{Z}_n^*|}_{\text{cardinality of } \mathbb{Z}_n^*}$ is called <u>Euler φ-function</u>.

Remarks:

- $\varphi(p) = p-1$, if p is prime.
- $\mathbb{Z}_n^*$ is a multiplicative Abelian group.

  $\gcd(a,n) = 1 \iff \exists$ inverse a^{-1} of a, s.t. $a^{-1}a \equiv 1 \pmod{n}$
- Notation $\gcd(a,n) = (a,n)$. If $(a,n) = 1$,

  a and n are called <u>relatively prime</u> or <u>coprime</u>.

<u>Theorem 6.2.</u> (Euler, Fermat)

If $a \in \mathbb{Z}_n^*$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$

In particular (Fermat's little theorem)

If p prime, $(a,p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$. ⊥

6.1. Probabilistic Primality Testing

Given $n \in \mathbb{N}$ (Call n <u>composite</u>, if n is not prime)

Question: Is n composite?

<u>FPT – Fermat Primality Test</u>

Select randomly some $a \in \{2, \dots, n-1\}$

Compute a^{n-1}.

$a^{n-1} \not\equiv 1 \pmod{n} \Rightarrow n$ composite

Otherwis declare "n prime"

Idea: If for composite n there are sufficiently many a with $a^{n-1} \not\equiv 1 \pmod{n}$, by independent repitition a high success prob. will be achieved.