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.
- An S-box is constructed as $x \mapsto x^{114} \in \mathbb{F}_2^8$.
  - 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 $\text{BC}_k$ 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 $\text{BC}_k$. Plaintext blocks $\text{M}_1, \text{M}_2, \text{M}_3, \ldots$

Encryption: $\text{C}_i = \text{BC}_k(\text{M}_i), i = 1, 2, \ldots$

Decryption: $\text{M}_i = \text{BC}_k^{-1}(\text{C}_i), i = 1, 2, \ldots$
5.4.2. CBC (cipher block chaining mode)

Given: Plaintext blocks $M_1, M_2, \ldots$

- Key $K$
- Initial vector (IV) $C_0$ (non-secret)

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

Decryption: $C_{i-1} \oplus M_i = \text{BC}^{-1}_K(C_i)$, hence

$$M_i = \text{BC}^{-1}_K(C_i) \oplus C_{i-1}, \ i = 1, 2, \ldots$$

5.4.3. CFB (counter feedback mode)

Given $(x)$, $z_0 = C_0$

Encryption: $z_i = \text{BC}_K(z_{i-1}), C_i = z_i \oplus z_i$

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

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

5.4.4. CFB (cipher feedback mode)

Given $(x)$

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

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

The key stream is dependent on the predecessor cipher block.
5.4.5 CTR (counter mode)

Given \( a \) \( Z_0 = C_0 \) (interpreted as some integer)

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

Decryption: \( M_i = B_k(Z_i) \oplus C_i, i = 1, 2, \ldots \)

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 \( C_u \) to the message \( (M_1 \ldots M_u) \)
  - If \( O/E \) tampers with the message, \( C_u \) does not fit any more.
- The authorized receiver, knowing \( k \), can easily verify \( C_u \); hence, verify the integrity or authenticity of \( (M_1 \ldots M_u) \)
Example. Storing passwords

- User types (name, password)
- System generates a key \( K = K(\text{name, password}) \)
  and stores \((\text{name, BC}_K(\text{password}))\)
- When logging in, system compares \((\text{name, \text{password}}) \) with the stored value.
Knowledge of \((\text{name, BC}_K(\text{password}))\) is useless for an intruder.

6. Number-Theoretic Reference Problems

Consider \( \mathbb{Z}_n \): ring of equivalence classes modulo \( n \)
\( s, t \in \mathbb{Z}, s \neq t \) or \( s \equiv t \pmod{n} \) \( \Rightarrow n \mid (s-t) \)
\( (\mathbb{Z}_n, \cdot) \) forms a ring. \( (\mathbb{Z}_n, \cdot) \) Abelian group,
\( (\mathbb{Z}_n, +) \) associative. 1 exists & distrib. laws.

Def. 6.1. \( \mathbb{Z}_n^{\ast} = \{ a \in \mathbb{Z}_n / \gcd(a, n) = 1 \} \)
is called the multiplicative group of \( \mathbb{Z}_n \).
\( \varphi(n) = |\mathbb{Z}_n^{\ast}| \) is called Euler \( n \)-function.
Cardinality of \( \mathbb{Z}_n^{\ast} \),
Remarks:
• $\phi(p) = p-1$, if $p$ is prime.
• $\mathbb{Z}_n^*$ is a multiplicative Abelian group.
• \[
gcd(a, n) = 1 \iff \exists \text{ an inverse } a^{-1} \text{ of } a, \text{ s.t. } a^{-1}a \equiv 1 \pmod{n}
\]
• Notation $\gcd(a, n) = (a, n)$. If $(a, n) = 1$, $a$ and $n$ are called relatively prime or coprime.

Theorem 6.2. (Euler, Fermat)
If $a \in \mathbb{Z}_n^*$, then $a^{\phi(n)} \equiv 1 \pmod{n}$

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 $n$ composite, if $n$ is not prime)

Question: Is $n$ composite?

FPT - Fermat Primality Test

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

Compute $a^{n-1}$. 

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

Otherwise declare "$n$ prime"

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