RWTH AACHEN UNIVERSITY

5.2.4. Design Considerations and Security

- After 2 rounds full diffusion is achieved, i.e., if 1 byte is modified in the input all 16 bytes of the output are modified.
- 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 about trapdoors (no mysteries about trapdoors)
- ShiftRows to resist 2 attacks: "truncated differentials" and "square attack"
- MixColumns causes diffusion
- Key schedule to avoid advantage from partial knowledge.
- Presently no better attacks than exhaustive search against AES 128.

  Attacks against AES 192 and AES 256 of complexity $\sim 2^{119}$

  see lecture notes.

Thinking the Future
Zukunft denken

RWTH AACHEN UNIVERSITY

5.3. Other block ciphers

- IDEA – Internat. Data Encryption Alg.
  - designed by Lai & Massey, 1990, Ascom, Switzerland
  - IDEA was part of PGP
  - Block length 64 Bits, key length 128 bits (description, see Schneier, p. 319)
  - IDEA is secure, best known attack exhaustive search
  - Patented in EU (1991), USA (1993) Non-commercial application are free.

- 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 operating on blocks of fixed length using key K.
5 modes of operations were standardized in Dec. 1980.

5.4.1. ECB (electronic code book mode)

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

Encryption: $C_i = BC_K(M_i)$, $i = 1, 2, \ldots$

Decryption: $M_i = BC_K^{-1}(C_i)$,

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)
$\Big\}$ (*)

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

(mimics the one-time pad)

RWTH AACHEN UNIVERSITY

5.4.4. CFB (cipher feedback mode)

Given (*)

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

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

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: " , $M_i = BC_K(Z_i) \oplus C_i$

Applications:

Example: MAC - message authentication code

In CBC and CFB modes, changing any plaintext block affects all subsequent ciphertext block.

Appropriate for generating a MAC.

- Append C_n to the message $(M_1, \ldots, M_n)$
- The authorized receiver, knowing K, can verify C_n. → integrity or authenticity of $(M_1, \ldots, M_n)$

Thinking the Future
Zukunft denken

<u>Example:</u> Storing passwords.

Direct storing of passwords is insecure. Hence:

- User types (name, passwd)
- System generates a key $K = K(\text{name}, \text{passwd})$ and stores $(\text{name}, BC_K(\text{passwd}))$
- When logging in, system compares $(\text{name}, BC_K(\text{passwd}))$ 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 classes mod n

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

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

$(\mathbb{Z}_n, +, \cdot)$ forms a ring

<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 $\mathbb{Z}_n$.

$\varphi(n) = \# \mathbb{Z}_n^*$ is called Euler-φ-function.

($\#$: order of $\mathbb{Z}_n^*$, no. of elements of $\mathbb{Z}_n^*$, cardinality)

<u>Remarks</u>

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

  It holds

  $\gcd(a,n) = 1 \Leftrightarrow \exists$ inverse s of a, i.e., $a \cdot s \equiv s \cdot a \equiv 1 \pmod{n}$.
- 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, $(a,p) = 1$ the $a^{p-1} \equiv 1 \pmod{p}$