AES, Feistel Networks, and Luby-Rackoff(1/2)

Douglas Wikström
KTH Stockholm
`dog@csc.kth.se`

February 3

- AES
- Feistel Networks
- Luby-Rackoff(1/2)

Quote of the Day

I believe that the Courtois-Pieprzyk work is flawed. They overcount the number of linearly independent equations. The result is that they do not in fact have enough linear equations to solve the system, and the method does not break Rijndael.

– Coppersmith, 2002

(about the XSL-attack of Courtois and Pieprzyk)

Advanced Encryption Standard (AES)

- Chosen in worldwide **public competition** 1998-2000. Probably no back-doors. Increased confidence!
- Winning proposal named “Rijndael”, by Rijmen and Daemen
- Family of 128-bit block ciphers:

Key bits	128	192	256
Rounds	10	12	14

- No attacks better than bruteforce (the XSL attack of Courtier and Pieprzyk is considered flawed), but...
- ... algebraics of AES make some people uneasy.

AES

1. **Initialization.** xor plaintext with round key.
2. **Normal Rounds.** (9, 11, or 13)
    1. Substitution: `SubBytes`
    2. Permutation: `ShiftRows`
    3. Linear Map: `MixColumns`
    4. xor With Round Key: `AddRoundKey`
3. **Last Round.**
    1. `SubBytes`
    2. `ShiftRows`
    3. `AddRoundKey`

Similar to SPN

- `SubBytes` is field inversion in $\mathbb{F}_{2^8}$ plus affine map in $\mathbb{F}_2^8$.
- `ShiftRows` is a cyclic shift of bytes with offset: 0, 1, 2, and 3.
- `MixColumns` is an invertible linear map with good diffusion.

Similar to SPN

- `SubBytes` is field inversion in $\mathbb{F}_{2^8}$ plus affine map in $\mathbb{F}_2^8$.
- `ShiftRows` is a cyclic shift of bytes with offset: 0, 1, 2, and 3.
- `MixColumns` is an invertible linear map with good diffusion.

Something like a mix between substitution, permutation, affine version of Hill cipher. In each round!

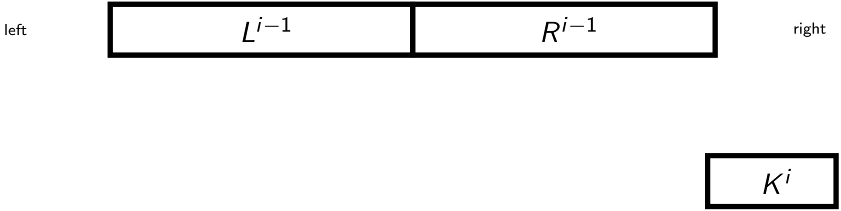
Feistel Networks

- Identical rounds are iterated, but with different round keys.
- The input to the *i*th round is divided in a left and right part, denoted L^{i-1} and R^{i-1}.
- f is a function for which it is somewhat hard to find pre-images, but f typically not neccessarily invertible!
- One round is defined by:

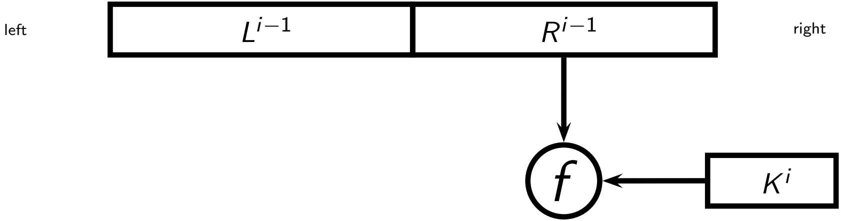
$$
\begin{aligned}
L^i &= R^{i-1} \\
R^i &= L^{i-1} \oplus f(R^{i-1}, K^i)
\end{aligned}
$$

where K^i is the *i*th round key.

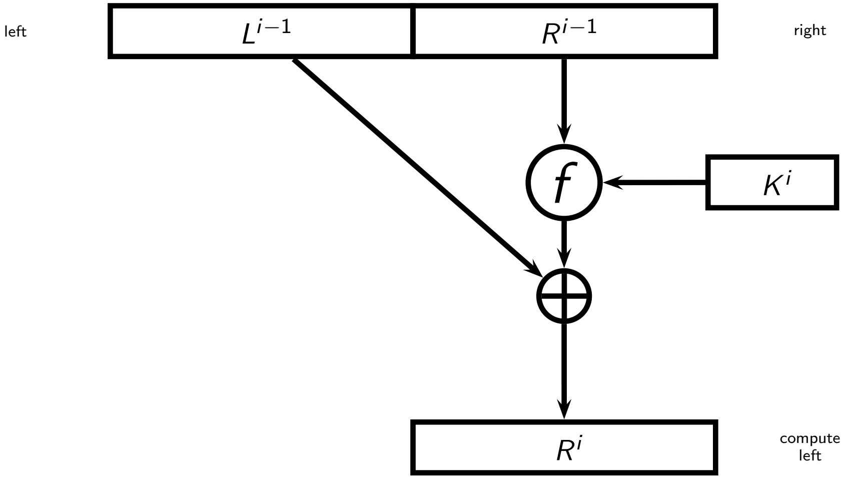
Feistel Round



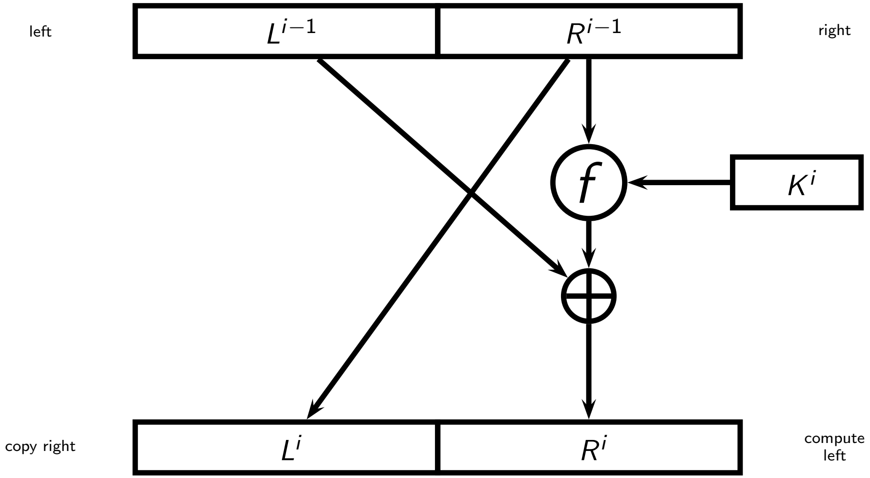
Feistel Round



Feistel Round



Feistel Round



Inverse Feistel Round

Feistel Round.

$$\begin{aligned} L^i &= R^{i-1} \\ R^i &= L^{i-1} \oplus f(R^{i-1}, K^i) \end{aligned}$$

Inverse Feistel Round

Feistel Round.

$$\begin{aligned} L^i &= R^{i-1} \\ R^i &= L^{i-1} \oplus f(R^{i-1}, K^i) \end{aligned}$$

Inverse Feistel Round.

$$\begin{aligned} L^{i-1} &= R^i \oplus f(L^i, K^i) \\ R^{i-1} &= L^i \end{aligned}$$

Reverse direction and swap left and right!

Negligible Functions

Definition. A function $\epsilon(n)$ is negligible if for every constant $c > 0$, there exists a constant n_0, such that

$$\epsilon(n) < \frac{1}{n^c}$$

for all $n \geq n_0$.

Motivation. Events happening with negligible probability can not be exploited by polynomial time algorithms! (they “never” happen)

Pseudo-Random Function

“Definition”. A function is pseudo-random if no efficient adversary can distinguish between the function and a random function.

Pseudo-Random Function

"Definition". A function is pseudo-random if no efficient adversary can distinguish between the function and a random function.

Definition. A family of functions $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is pseudo-random if for all polynomial time oracle adversaries A

$$\left| \Pr_K \left[A^{F_K(\cdot)} = 1 \right] - \Pr_{R:\{0,1\}^n \to \{0,1\}^n} \left[A^{R(\cdot)} = 1 \right] \right|$$

is negligible.

Pseudo-Random Permutation

"Definition". A permutation and its inverse is pseudo-random if no efficient adversary can distinguish between the permutation and its inverse, and a random permutation and its inverse.

Pseudo-Random Permutation

“Definition”. A permutation and its inverse is pseudo-random if no efficient adversary can distinguish between the permutation and its inverse, and a random permutation and its inverse.

Definition. A family of permutations $P : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ are pseudo-random if for all polynomial time oracle adversaries A

$$\left| \Pr_K \left[A^{P_K(\cdot), P_K^{-1}(\cdot)} = 1 \right] - \Pr_{\Pi \in \mathcal{S}_{2^n}} \left[A^{\Pi(\cdot), \Pi^{-1}(\cdot)} = 1 \right] \right|$$

is negligible, where $\mathcal{S}_{2^n}$ is the set of permutations of $\{0,1\}^n$.

Idealized Four-Round Feistel Network

Definition. Feistel round (H for "Horst Feistel").

$$H_{F_K}(L, R) = (R, L \oplus F(R, K))$$

Idealized Four-Round Feistel Network

Definition. Feistel round (H for "Horst Feistel").

$$H_{F_K}(L, R) = (R, L \oplus F(R, K))$$

Theorem. (Luby and Rackoff) If F is a pseudo-random family of functions, then

$$H_{F_{k_1}, F_{k_2}, F_{k_3}, F_{k_4}}(x) = H_{F_{k_4}}(H_{F_{k_3}}(H_{F_{k_2}}(H_{F_{k_1}}(x))))$$

(and its inverse) is a pseudo-random family of permutations.

Idealized Four-Round Feistel Network

Definition. Feistel round (H for "Horst Feistel").

$$H_{F_K}(L, R) = (R, L \oplus F(R, K))$$

Theorem. (Luby and Rackoff) If F is a pseudo-random family of functions, then

$$H_{F_{k_1}, F_{k_2}, F_{k_3}, F_{k_4}}(x) = H_{F_{k_4}}(H_{F_{k_3}}(H_{F_{k_2}}(H_{F_{k_1}}(x))))$$

(and its inverse) is a pseudo-random family of permutations.

Why do we need four rounds?