Stream Cipher—RC4

Stream ciphers don't encrypt PT blocks directly.

Used in some version of cellular communication traffic. Invented in 1987 by Rivest. Posted on the Cypherpunks mailing list in 1994.

Seed: A permutation of the sequence $(0 \ldots 255)$ and two numbers $0 \leq i, j < 256$.

```
do forever: i = (i+1) % 256
            j = (j + S[i]) % 256
            swap(S[i], S[j]) --- update register state
            t = (S[i] + S[j]) % 256
            output S[t]
```

Is it secure? Can't prove it. Are there weak keys for RC4?

1997: Run generator for 10^{12} iterations. LSb of these 10^{12} bytes has slightly more 1's than 0's.

Symmetric Key Systems

Adapted from [Pfl96, Section 3.8].

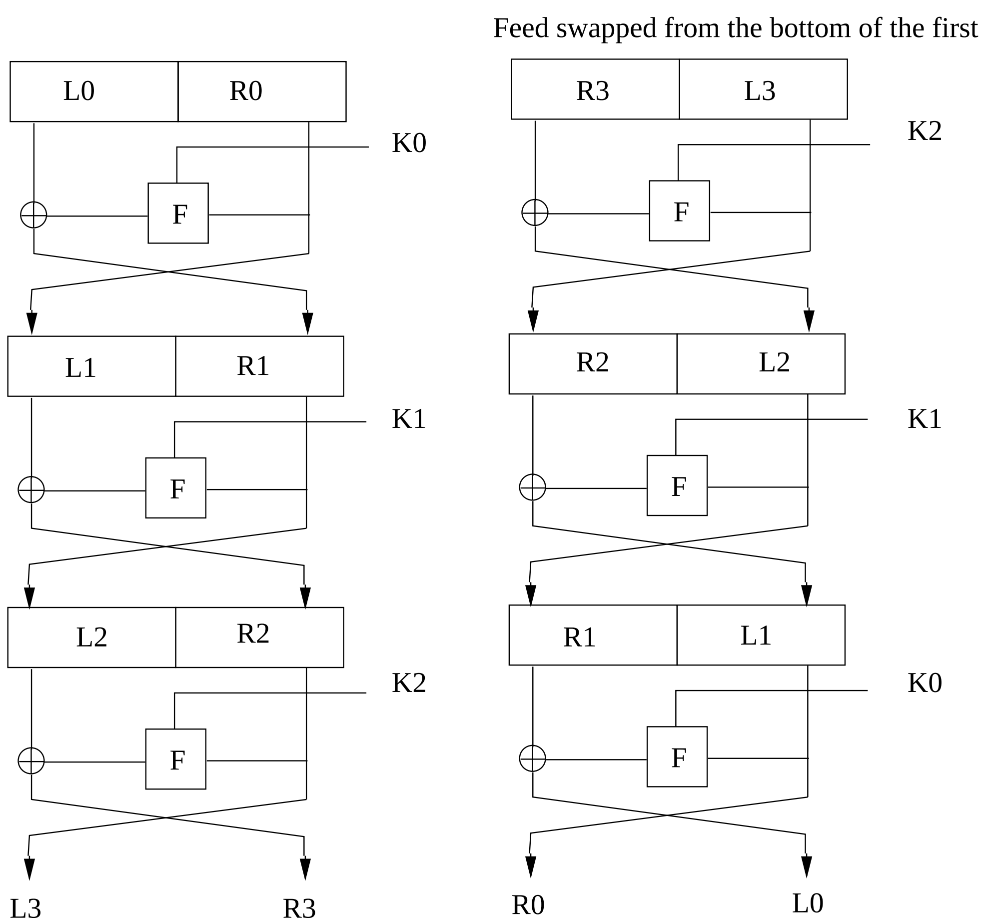
- Single key systems are called **secret key** or **symmetric** encryption systems.
- As long as the key remains secret, the system also provides **authentication**. Encrypt $\boxed{m \mid \text{h(m)}}$ with the shared secret.
- If the key is revealed, all communication is exposed. Change keys frequently.
- Key distribution becomes a problem. Split the key into pieces and send through separate mechanisms.
- Number of keys required for n party communication is $O(n^2)$ directly, or $O(n)$ through a trusted third party.

Feistel Cipher Structure

See [Sta99, Fig. 3.5].

- Substitution and Permutation in each round.
- Decryption essentially same as encryption.
- Parameters: block size, key size, # of rounds, key schedule, round function.
- Other Considerations: Fast software encryption/decryption, Ease of analysis.

A Feistel structure inverts its own output with a reverse key schedule.



DES

Described in FIPS46-3.

History:

- Late '60s Feisel worked on block ciphers.
- 1972 NBS (NIST) issued RFP.
- 1974 IBM developed and submitted LUCIFER (64 bit block, 128 bit key).
- NSA "fixed" it (S-boxes).
- 1979 Adopted as a standard, accepted by the banking community.
- 1999 Broken in 22 hours using exhaustive key search.

Properties:

- Block size $= 64$ bits; key size $= 56$ bits.
- Software nightmare because of permutations and table lookups.
- Great for pipelining because each round can work on a different key.
- Key size too short—brute force search possible.
- Exhibits strong avalanche effect [Sta99, pg. 73].
- $\overline{DES_k(X)} = DES_{\overline{k}}(\overline{X})$.
- $\exists$ keys k in DES such that $DES_k(m) = DES_k^{-1}(m)$. These are called weak keys. These are keys that generate a key schedule in which
$$k_1 = k_2 = \cdots = k_{16}$$
- $\exists$ keys k, k' in DES such that $\forall m,\ DES_k(m) = DES_{k'}(m)$. These are called semi-weak keys.

Show my m4 diagram of propagating L_0, R_0 to L_{16}, R_{16}.

Avalanche effect: $\triangle$ PT or Key $\Rightarrow \bigtriangleup$ in CT.

Block Cipher Modes

ECB. $C_i = E_k(M_i)$. It's **malleable** i.e., an active intruder can swap C_i and C_j or compose whole messages from parts of separate ones, as in for e.g., [Pfl96, Section 4.4].

Depositor	Account #	Amount
$24B$	$8B$	$8B$

CBC. $C_i = E_k(M_i \oplus C_{i-1})$.

- IV is secret because initial parts of the message may be known, such as e-mail headers etc., which would provide a (M, C) pair.
- A transmission error affects at most two plain text blocks, the block containing the error and the following one.
- Decryption: $M_i = D_k(C_i) \oplus C_{i-1}$

OFB. $C_i = P_i \oplus E_k^i(IV)$. Turns DES into a stream cipher-like mode. Both IV and K are secret. Nobody uses it because there are much faster stream ciphers. Transmission bit errors do not propagate.

CFB. $C_i = P_i \oplus E_k(C_{i-1})$. A transmission error affects at most two plain text blocks in this case as well. $P_i = C_i \oplus E_k(C_{i-1})$.

So it seems that a transmission error affects at most two plaintext blocks in this case as well.

Attacks on Block Ciphers—Exhaustive Search

Try all possible keys. 2^{56} keys $\approx 10^{19}$ keys.

Cost	Time
1 DES encryption/μs	> 1000 years
Wiener \$100K machine	35 hours
Wiener \$1 M machine	3.5 hours $= 210$ mins
Wiener \$10M machine	21 mins

Attacks on Block Ciphers—Differential Cryptanalysis

Biham & Shamir 1989. $O(2^{47})$ time and $O(2^{47})(M, C)$ pairs on DES. If the S-boxes were random, a differential cryptanalytic attack would require $O(2^{20})$ time and $O(2^{20})(M, C)$ pairs.

DES Variants—Double-DES

If $E_k(M)$ is a symmetric cipher, then define

$$\text{DE}_{k_1,k_2} = E_{k_1}(E_{k_2}(M))$$

- Pictorially, it is $M \longrightarrow \boxed{E_{k_2}} \longrightarrow \boxed{E_{k_1}} \longrightarrow C$.
- Susceptible to *meet-in-the-middle* attack. Given an (M, C) pair:
  Step 1: Build the following table for all keys k

k_1	$E_{k_1}(M)$
k_2	$E_{k_2}(M)$
k_i	$E_{k_i}(M)$

  Step 2: $\forall k$, check if $E_k^{-1}(C)$ is in the table. For a k bit key, time $\approx 2^k + 2^k \cdot \log 2^k \approx k \cdot 2^k$.

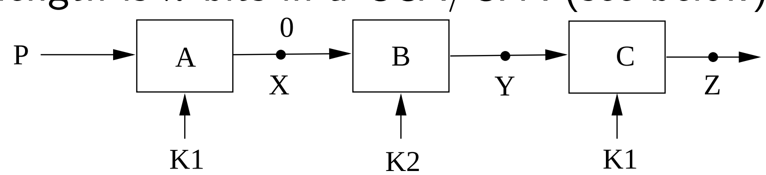
  That is, given <u>enough space</u>, DE is only as secure as E.

DES Variants—Triple-DES

If $E_k(M)$ is a symmetric cipher, then define

$$\mathsf{2KTE}_{k_1,k_2} = E_{k_1} \circ D_{k_2} \circ E_{k_1}$$

- Key length $= 112$ bits.
- D_{k_2} only for backward compatibility, could use E instead.
- Effective key length is k bits in a CCA/CPA (see below).



  For all keys k compute $D_{k_2}(0)$ in a table T. Now, for each key k, find $p = D_k(0)$. Do a CPA on p to find the corresponding z. From this z, k find y. See if y occurs in T. This is a possible pair of keys for T-DES.

  Except for an uncommon attack noted by Merkle, triple DES does yield the expected strength of 2^{112} [Pfl96, Section 4.5].

- Better to use three independent keys.

$$\mathsf{TE}_{k_1,k_2,k_3} = E_{k_1} \circ D_{k_2} \circ E_{k_3}$$

  Effective key length $= 112$ bits in a KPA (meet-in-the-middle).

How to Use Encryption

Adpated from [Pfl96, Section 4.3].

- The degree of secrecy needed should determine the amount of labor appropriate for encryption and decryption.
- Delay to Encrypt
  - Block cipher (wait for block to fill) or Stream cipher.
  - Latency resulting from key schedule generation.
- Size of Ciphertext—Block cipher (padding and concomitant expansion) or Stream cipher.
- Encryption alone does **not** provide integrity.

Uses of Encryption

Adpated from [Pfl96, Section 4.4].

- One way functions for passwords.
- Integrity via $E(m||h(m))$.
- Authentication via $E_k(m||h(m))$ with k that you share with a known person.
- Timestamps and integrity for preventing replay. Use $E_k\left(\boxed{m \mid t \mid h(m||t)}\right)$ for replay protection and integrity.

References

[KR96] Joe Killian and Phillip Rogaway. How to protect des against exhaustive key search. *Proceedings of Crypto 96*, 1996.

[Mat93] Mitsuru Matsui. Linear cryptanalysis method for des cipher. *Proceedings of Eurocrypt*, 1993.

[Pfl96] Charles P. Pfleeger. *Security in Computing*. Prentice Hall, iind edition, 1996.

[Sta99] William Stallings. *Cryptography and Network Security*. Prentice-Hall Inc., 2nd edition, 1999.

[WT85] A. F. Webster and S. E. Tavares. On the design of s-boxes. *Advances in Cryptography—Crypto '85*, 1985.

If a cryptographic transformation is *complete*, then each ciphertext bit must depend on all the plaintext bits. Thus, if it were possible to find the simplest boolean expression for each ciphertext bit in terms of the plaintext bits, each of the expressions would have to contain all of the plaintext bits if the function was *complete*.