Symmetric Encryption. Feistel cipher and DES family

NSE, sections 2.1-2.2
WSPC, chapter 3

Analysis vs cryptanalysis

- One of the main goals when creating new encryption/decryption algorithm is to make it as difficult as possible for *cryptanalysis* (difficult to break);
- One the other hand, making an algorithm easy to *analyse* could be beneficial, because then
  - Analysis of the algorithm can provide with a higher level of assurance;

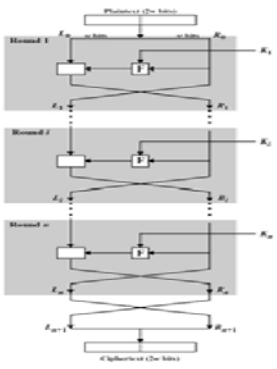
Block vs stream ciphers

- **The way in which plaintext is processed**
  - Block cipher: input block of elements (e.g. characters) is transformed to the output block at once;
  - Stream cipher: processes the input elements continuously, one element at a time.

Feistel cipher structure

- Most symmetric block encryption algorithms have a structure proposed by H.Feistel in 1973;
- The input is divided into the blocks of even numbers of elements;
- Then multiple stages of substitutions and transpositions is applied;
- Multiple keys (derived from a single key) are used at different rounds of the algorithm.

Feistel Cipher Structure



- Input is a plaintext block of the size 2w bits;
- The block is divided into two parts L_0 and R_0;
- Two parts going through n rounds of processing;
- At every round, a function F (round function) is applied to the right half using a (sub)key, the result is XOR'ed with the left half of the data;
- At every round a new (sub)key may be used; all sub(keys) are generated from the same secret key

Decryption in a Feistel cipher

- The same algorithm is used as for encryption;
- The only difference is subkeys should be applied in a reverse order:
  - If for encryption $K_1,\ldots K_n$ have been used at the rounds 1, …,n, then
  - $K_n,\ldots,K_1$ are used for decryption at the rounds 1,..n.

Choices in Feistel network scheme

- **Block size:** the larger the block size the more secure and slower the scheme is. 64 bits is a usual size;
- **Key size:** the larger key size means the greater security but slower the scheme. 128 bits is the most common key length;
- **Number of rounds:** more rounds means more security;
- **Subkey generation algorithm:** more complex algorithm generally means more difficult cryptanalysis;
- **Round function:** the same as above.

Symmetric Encryption Algorithms

Most important symmetric block ciphers

- DES (Data Encryption Standard);
- 3DES (triple DES);
- AES (Advanced Encryption Standard);

Data Encryption Standard (DES)

- Adopted in 1977 by National Bureau of Standards (now NIST);
- The algorithm itself is called Data Encryption algorithm (DEA);
- A variant of the Feistel schema;
- Blocks have a size 64-bits;
- The key is 56 bits long;
- Uses 16 rounds of processing;
- From the original 56-bit kay, 16 subkeys are generated, one for each round.

The weakness of DEA

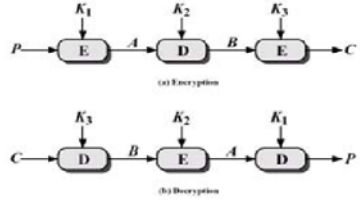
- **Weakness:** the size of the key (56 bits).
  Altogether there are $2^{56} \approx 7.2 \times 10^{16}$ different keys of such a length;
- The number is huge, but the special purpose machine "DES cracker" built in 1998 was able to break the algorithm in a less than 3 days using brute-force search;
- **Remedy:** increase the length of the key!! Increasing the length to 128 bits would increase the time of the brute-force search by "DES cracker" to 10^{18} years.

The strength of DEA

- The strength of DEA is based on the fact that no essentially better than brute-force search attack is known for DEA;
- In other words, no fatal weakness of DES itself has been discovered (only the weakness related to the small length of the key);
- But, no proof that an efficient attack is impossible.

Triple DES

- Triple DES (3DES) is a standard introduced in 1985;
- 3DES algorithm does what its name says: it runs DES (rather DEA) algorithm 3 times;
- It uses three keys, one for each execution of DEA;



Encryption and Decryption in 3DES

Encryption: $C = E_{K_3}[D_{K_2}[E_{K_1}[P]]]$

Decryption: $P = D_{K_1}[E_{K_2}[D_{K_3}[C]]]$

Where

- C is ciphertext
- P is plaintext
- $E_K[X]$ is encryption of X using key K
- $D_K[Y]$ is decryption of Y using key K

3DES is compatible with DES: $C = E_{K_1}[D_{K_1}[E_{K_1}[P]]] = E_{K_1}[P]$

Advanced Encryption Standard

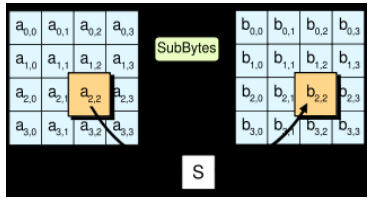
- Designers: J. Daemen, Vincent Rijmen
- First published: 1998
- Became effective as a NIST standard May, 2002
- A variant of substitution-permutation network
- Key size is 128, 192 or 256 bits
- Number of rounds is 10, 12, or 14

Advanced Encryption Standard

- Design uses theory of finite fields, a branch of algebra;
- Every block of 128 bits is presented as 4 by 4 array of bytes
- Key Expansion: Key → Round keys

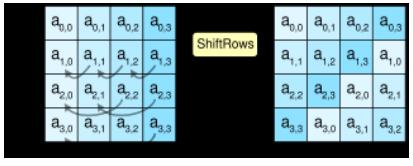
Steps in AES processing, I

- Every round includes the following steps:
  - **Substituiton**: each byte is replaced with another based on lookup table



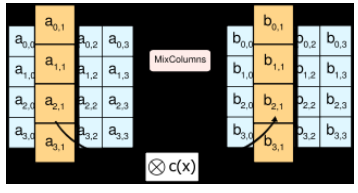
Steps in AES processing, II

– **ShiftRows**: each row is shifted cyclically certain amount of steps



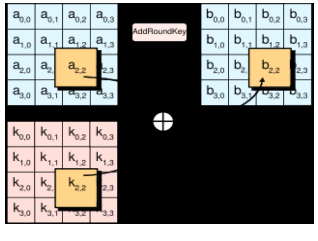
Steps in AES processing, III

– **MixColumns:** mixing operation on the columns (defined in terms of computations in a finite field).



Steps in AES processing, IV

– **AddRoundKey-** each byte is combined with the round key



Security of AES

- Considered secure for use for classified information, secret and top secret level;
- However, there are some concerns related to the algebraic foundations of algorithm – underlying algebraic structure might be used in the attacks in some clever way;
- For more details see Wikipedia entry on AES