Class278: Block ciphers and modes of operation

Virendra Sule

August 26, 2020

1 Block ciphers

We saw in previous discussion that a Stream cipher generates a PR stream of alphabets $\{k_i\}$ and encrypts a plaintext stream of alphabets $\{p_i\}$ as the ciphertext stream

$$\{c_i\} = \{p_i \oplus k_i\}$$

The key stream is generated through a state update and output maps $F : X \to X$ and $f : X \to A$.

Block ciphers are algorithms which have as inputs a block of plaintext and key. A block cipher takes in a stream of blocks of plaintext alphabets P_i, $i = 1, 2, 3, \ldots$ and generates blocks of ciphertext C_i by means of the Encryption function

$$C_i = E(K, P_i)$$

where K is the same key block used for each input P_i. Consider the alphabet set A to be the binary field $\mathbb{F}_2$ and let n denote the block length. Then each of the blocks P_i, K and C_i are strings of n bits. The block cipher satisfies following conditions.

1. Encryption function $C = E(K, P)$ is a TOWF with trapdoor K which is called the symmetric key.
2. The inverse of C when K is known is denoted as the decryption function

   $$P = D(K, C)$$

   which is also a TOWF with trapdoor K. Hence the two functions E and D satisfy

   $$E(K, D(K, C)) = C, D(K, E(K, P)) = P$$

   i.e. they are inverses of eachother. Depending on the way (mode) of operation of the cipher, the block cipher may be given as only the algortihm E or as both E and D

Block cipher is required for bulk encryption when the plaintext consists of a sequence of blocks

$$\hat{P} = \{P_1, P_2, \ldots, P_m\}$$

of alphabets. Since the key used for encrypting each block is same, if there is correlation between blocks P_i, P_{i+1} or some other block P_j, then a correlation may appear in C_i and C_j. Hence it may be possible to distinguish which blocks are encrypted. Hence a stonger requirement of confidentiality of encryption is *indistinguishability.* Although the TOWF property does not allow computation of C given P without K the correlation may allow recognising which block is encrypted. Hence block ciphers need to be used in specific modes of operation.

1.1 Block cipher construction by substitution and permutation (SP) networks

A standard way of constructing a TOWF is by following processes:

1. Substitution of alphabets. Since an input block P to the encryption function consists of a string of n alphabets,

   $$P = (p_1, p_2, \ldots, P_n)$$

   if $S : A \to A$ is a permutation of the set of alphabets, define the substitution on blocks by $\hat{S}$

   $$\hat{S} = (S(p_1), S(p_2), \ldots, S(p_n))$$

2. Permutation of sub-blocks. Let P has multiple sub-blocks

   $$P = (B_1, B_2, \ldots, B_l)$$

   and Π is a permutation

   $$\Pi = \left(\begin{array}{llll} 1 & 2 & \ldots & l \\ \Pi(1) & \Pi(2) & \ldots & \Pi(l) \end{array} \right)$$

   Then define

   $$\Pi(P) = (B_{\Pi(1)}, \ldots, B_{\Pi(l)})$$

3. Mixing of the key. A mixing of the key and its expansion using the above operations into an intermediate block X by

   $$X \oplus K = (X_1 \oplus K_1, \ldots, X_n \oplus K_n)$$

Several steps or rounds of such operations can be used to create a practical TOWF. According to Shannon, an encryption function must involve sufficient amount of *confusion*, *diffusion* and *mixing* of randomness. Confusion is caused by substitution when the alphabet set is sufficiently large such as of 256 elements. While diffusion refers to diffusion of information which is brought about by permutation of sub-blocks. By permuting sub-blocks local correlations between sub-blocks of the language get diffused or distributed. Similarly mixing of a random key with any interim block adds the randomness associated with the key which causes mixing of randomness. Practical TWOF are created by such operations. However they are secure from a computational viewpoint only if the length of the block is sufficiently large and sufficient rounds of substitution, permutation and mixing are carried out. A formal way of proving the difficulty of compromising a TOWF is usually not available. Hence a cipher is considered secure if no approach better than brute force search over key is known for breaking the third property and the brute force search is practically not feasible.

Example 1. Consider the alphabet set to be $\{A, B, C, D, E\}$ with $\oplus$ as a modulo 5 sum of order of these letters with $A = 0$. Consider a plaintext block

$$P = (EDBBCADAEABE)$$

Consider a substitutiton map

$$S(A) = C, S(B) = A, S(C) = D, S(D) = E, S(E) = B$$

Then $S(P) = (BEAADCECBCAB)$. If $\Pi(1, 2, 3, 4) = (4, 1, 3, 2)$ and consider blocks of three alphabets in P then

$$\Pi(P) = (ABEEDBDAEBCA)$$

If $K = (DCBBEACDACDE)$ then

$$P \oplus K = (CACCBAAAECED)$$

1.2 Modes of operation of Block ciphers

Following are standard modes recommended for using a block cipher.

1. Electronic Code Book (ECB): Each plaintext block is encrypted separately as above,

   $$C_i = E(K, P_i)$$

   The ciphertext transmitted is the sequence C_i, $i = 1, 2, \ldots, m$. Decryption is done by

   $$P_i = D(K, C_i)$$

   This mode is unsatisfactory since it does not give indistinguishability.

2. Cypher Block Chaining (CBC): The ciphertext clock is affected by previous block. Let $C_0 = IV$ is an initial block chosen randomly

   $$C_i = E(K, P_i \oplus C_{i-1})$$

   for $i = 1, 2, \ldots, m$. The ciphertext transmitted is C_j for $j = 0, 1, 2, \ldots, m$. Decryption is done by

   $$P_i = D(K, C_i) \ominus C_{i-1}$$

3. Cipher Feedback mode (CFB): Let the block itself be divided into sub-blocks of fixed length. For a general block of 64 bits denote $P = P_1P_2 \dots P_8$. Say over $\mathbb{F}_2$ each sub-block is of 8 bits. An initial vector IV, X of 64 bits is chosen. $L_8(X)$ denotes leftmost 8 bit su-block of X while $R_{56}(X)$ is the right sub-block of 56 bits. Then define encryption by following for $j = 1, 2, \dots$
$$\begin{array}{lcl} Q_j & = & L_8(E(K, X_j)) \\ C_j & = & P_j \oplus Q_j \\ X_{j+1} & = & R_{56}(X_j)||C_j \end{array}$$
thus a previous sub-block of ciphertext is used in defining the next sub-block. The initial vector X is sent along with the ciphertext C. Decryption is done in terms of sub-blocks
$$P_j = C_j \ominus Q_j$$
Thus the decryption function is not used in this mode.

4. Output Feedback mode (OFB): An IV X is chosen and encryption is carried out as follows:
$$\begin{array}{lcl} Q_j & = & L_8(K, X_j) \\ X_{j+1} & = & R_{56}(X_j)||Q_j \\ C_j & = & P_j \oplus Q_j \end{array}$$
OFB also does not use the decryption function.

5. Counter mode (CTR): This mode shows that actually a block cipher can be used to generate a stream of blocks and hence can be used as a stream cipher but not strictly by state update map. First an IV block X_0 is chosen randomly. This corresponds to a number if the bits of X_0 denote the binary expansion of the number. This number is incremented by one at each time index of the stream
$$\begin{array}{lcl} X_j & = & X_{j-1} + 1 \text{ integer addition} \\ Q_j & = & E(K, X_j) \\ C_j & = & P_j \oplus Q_j \end{array}$$
Again in CTR mode the decryption function is not used.

In all the feedback schemes and CTR scheme above, the 8 bit sub-block can be taken as full block. As an exercise write these formulas.

1.3 Attacks on Block ciphers

An attack on a cipher is a methodology of ascertaining strength of the TOWF of the block cipher. First note that the key space, the input space of plaintext blocks are both finite sets. Hence in principle the third property of the TOWF that of finding K given P and C blocks never holds if we consider the brute force search over all keys K, as given C for a block P we can search through all possible keys K such that $E(K, P)$ matches C. However for a K of n-bits such a search to match C involves 2^n distinct trials of K. Hence the brute force search is infeasible for sufficiently large n. Hence the encryption function is a TOWF when there is no other simpler search possibly known. The attacks are scenarios in which functionality of the TOWF is compromised. Primary attacks are as follows. Every attack assumes that the attacker has full knowledge of the TWOF but does not have the key K:

1. Ciphertext only attack. In this attack, the attacker has the ciphertext and tries to find either or both of K and P. In a monoalphabetic cipher the density of letters or double letters in a languge allows recognition of the plaintext from ciphertext. A cipher in which the OWF property of discovering P from C computationally fails is never used in modern encryption.

2. Known plaintext attack. In this attack, the attacker has pairs P, C of a few known plaintext blocks P and their ciphertext blocks C. The attacker tries to solve for the key K knowing the encryption function. In practical situation this attack is feasible due to knowledge of some parts of plaintext (such as known structure, date and phrases in a letter). Since this function involves several rounds of substitution, permutations and key mixing, an algorithm better than brute force search over K is difficult to construct for a good encryption function.

3. Chosen plaintext attack. Attacker can choose the plaintext and ask for the ciphertext. This attacks also follows from the attack on the decryption function by giving a random string to be decrypted as it happens in an identification of friend or foe. By choosing the plaintext based on previously known plaintext such an attack can be made adaptive to history of plaintext.

4. Chosen ciphertext attack. This version is similar to the chosen plaintext attack for the decryption function. Applicability of such an attack is more relelvant in asymmetric encryption.

5. Distinguishability attack. In this attack case the attacker gives two plaintexts P_0, P_1 of her choice and asks for ciphertext of one of them. Then using knowledge of the encryption function determines which of the two plaintext was encrypted.

If $C = E(K, P)$ is the encryption function then for a known plaintext block P the ciphertext block C defines a system of equations in which bits of K are the only unknowns. But this system of equations is non-linear. Solving such systems in the attack scenarios are hard problems of computation. The TWOF is also required to pass the distinguishability attack. Making estimates of time, memory, complexity of the attack problems under different scaled models of the TOWF is a necessary and independent subject called *Cryptanalysis*. Hence cryptanalysis of a cipher is necessary to pass a cipher for practical use.