CS557: Cryptography

Modern Ciphers

S. Tripathy
IIT Patna

Previous Class

- Cryptology
  - Cryptography and Cryptanalysis
    - Classical Ciphers

Some Security Definitions

- computational security
  - given limited computing resources, the cipher cannot be broken
- unconditional security
  - no matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext

- Provable Security
  - Provide evidence of security by reducing the security of the cryptosystem into a well studied problem

An unconditionally Secure Cipher

- Vernam Cipher
  - Gilbert Vernam invented and patented his cipher in 1917 while working at AT&T
  - also known as the one-time-pad.
- Encryption
  - plaintext + key = ciphertext
- Decryption
  - ciphertext - key = plaintext

- Veernam's One-Time Pad
  - A truly random key as long as the message is used called a One-Time pad
  - is unbreakable since ciphertext bears no statistical relationship to the plaintext
  - since for *any plaintext* & *any ciphertext* there exists a key mapping one to other
  - can only use the key *once* though

- have problem of safe distribution of key

Perfect Secrecy

- *Definition*: A Cryptosystem has *perfect secrecy* if

  $P(E(k,m1)=c) = P(E(k,m2)=c)$

Shanon's secret cipher

$p(M=m|C=c) = p(M=m)$ for all plaintexts m and all ciphertexts c.

- *Lemma*: Assume the cryptosystem is *perfectly secure*, then

  $|K| \geq |C| \geq |M|$,

  where $|X|$ denotes the size of the set of possible x

NB: The concept of perfect secrecy is restricted to a situation where key is used for only one encryption.

Entropy: Measure of uncertainty concept (shanon 1948)

Ex: Shift cipher (with length=1) maintains perfect secrecy?

- $Pr(m \mid c) = pr(m)\, pr(c|m) / pr[c]$

- $pr[c] = \sum pr(k=K) pr(m=d_k(c))$
- $= \sum 1/26\ pr(m=c-k) = 1/26 \sum pr(m=c-k) = 1/26$

  – Since for each k there would be one and only one m to c

  i.e. $\sum pr(m=c-k) = 26\ (1/26) = 1$ so $pr[c] = 1/26$

- Again $pr(c|m) = pr(k= c-m \pmod{26}) = 1/26$

- $Pr(m \mid c) = pr(m)\, pr(c|m) / pr[c] = (pr(m).\ 1/26)$
- $=pr(m)$

Product Ciphers

- Uses a sequence of substitutions and transpositions
  - Harder to break than just substitutions or transpositions

- This is a bridge from classical to modern ciphers.

Modern Ciphers

- We design one relatively simple scrambling method (called a round) and repeat it many times

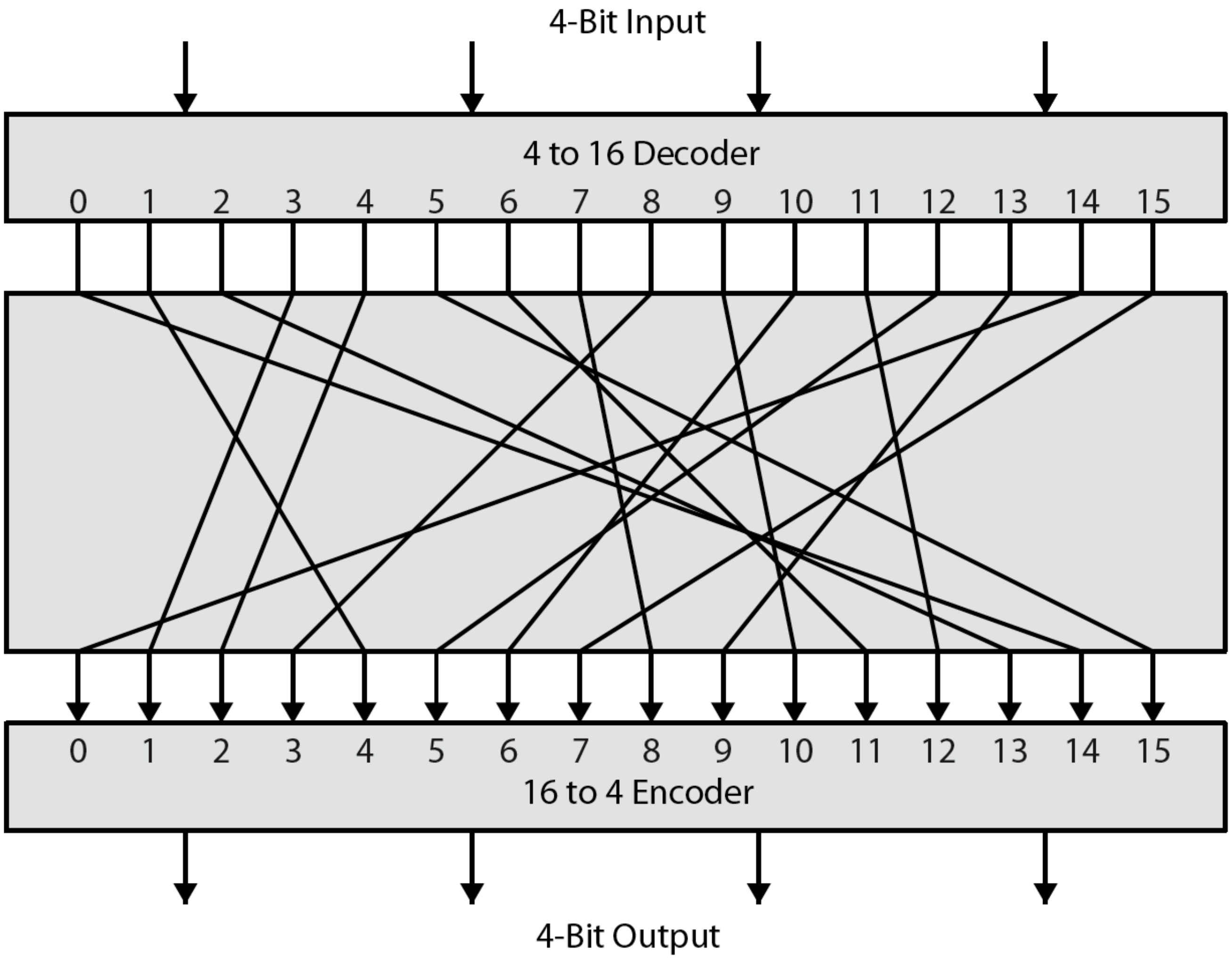
  - One round may be easy to break, but when you put them all together it becomes very hard

- Almost all ciphers follow one of two structures
  - SPN (Substitution Permutation Network)
  - Feistel Network (basis for DES)
  - These describe the basic structure of a round

Block cipher

- An encryption function: $E = \{E_k\}$ is a family of 2^l permutations on n bits indexed by K, where K is l bits
- A decryption function: $D = \{D_k\}$ is a family of 2^l permutations on n bits indexed by k such that D_k is the inverse of E_k.
- Given a n-bit plaintext, P, and key, k, if $C = E_k(P)$ then $P = D_k(C)$.

Ideal Block Cipher



2-bit Block cipher

- Consider a block of size 2-bit.
- 24 different permutations
  - so 5-bit keys

k=00000

P	C
00	10
01	11
10	01
11	00

k=00001

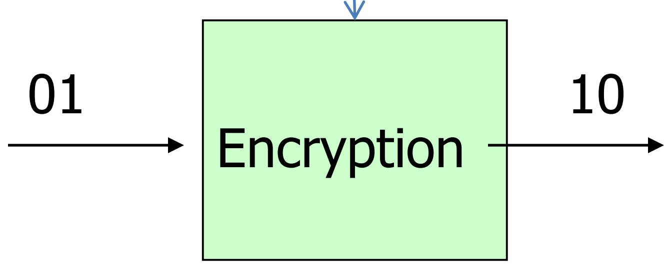
P	C
00	11
01	00
10	01
11	10

k=00010

P	C
00	11
01	10
10	01
11	00

k=00011

P	C
00	01
01	00
10	11
11	10



Block cipher

- Length of the key?
- # n-bit permutations in block cipher: $2^n!$
  -
- Design aim: choose the 2^l permutations uniformly at random from the set of all $2^n!$ Permutations
- Aim of Cryptanalysis:
  - find key k, or find (m, c) such that ek (m) = c for unknown k, or
  - distinguish member of block cipher from randomly chosen permutation

Block cipher Design Principle

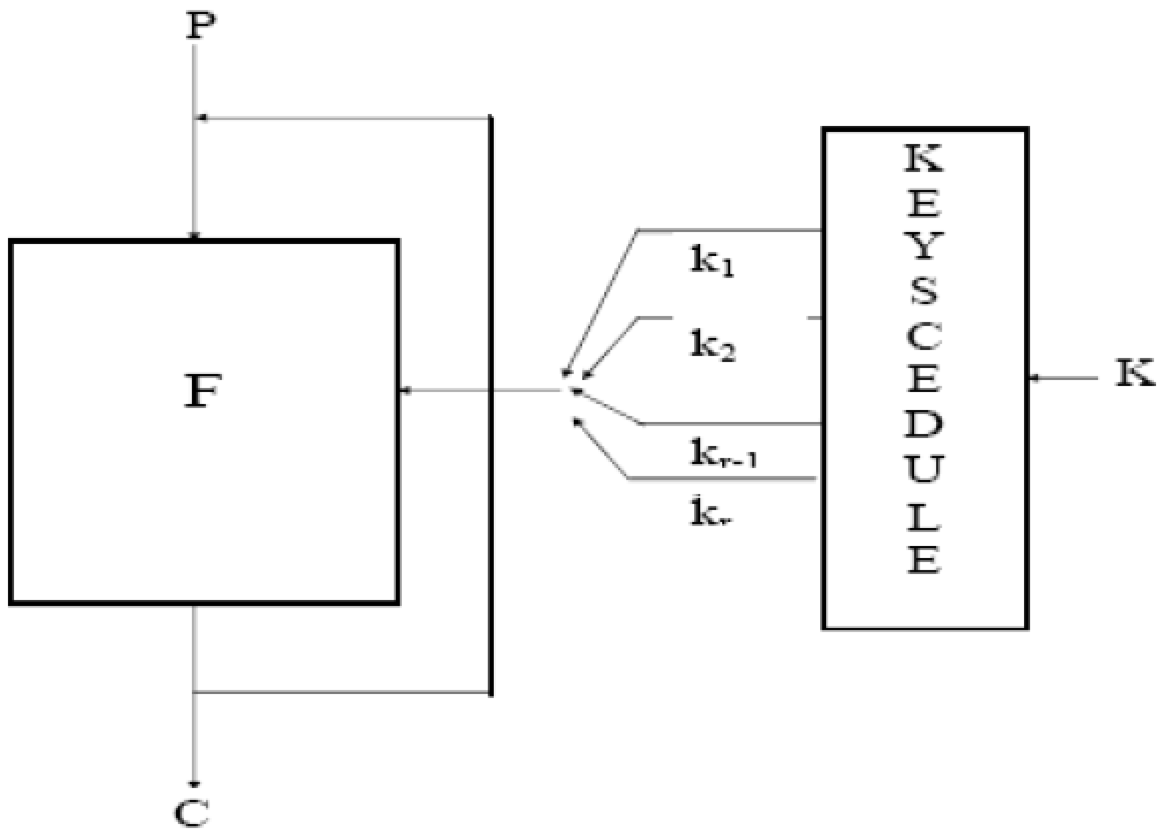
- Confusion:
  - The relation between the statistics of cipher text and plain texts must be complex
- Diffusion:
  - Every bit of the cipher text should depend on the every bit of key and plain text

Ex.: Suppose encrypting plaintext 1111111111111111 produces ciphertext 0110110000101001

Then encrypt 1111111011111111, can't predict anything about ciphertext

- These two important properties can be achieved by repeatedly using of keyed substitutions and permutations.
  - Block cipher in this principle is called Iterated Block cipher

Iterative Block cipher



Iterated Block cipher

- E(K, p)
- {
- (K1, . . .KNr) <-- Ks(K)
- w0 <-- p
- for i <-- 1 to Nr do
- wi <-- F(wi–1,Ki–1)
- c <-- w_{Nr}
- Return (c)
- }

- D(K, c)
- {
- (K1, . . .KNr) <-- Ks(K)
- w0 <-- p
- for i <-- 1 to Nr do
- wi <-- F^{-1}(wi–1,Ki–1)
- c <-- wNr
- Return (c)
- }

Common Building Blocks

Substitution-Permutation Network (SPN)

- General term for sequence of operations that performs substitutions and permutations on bits

Feistel Network (will see example later)

- For input $L_0 || R_0$ and any function F
- $L_i = R_{i-1}$
- $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$
- K_i = other input to F, (ex. key material)

Whitening

- XOR data with key material ($X \oplus K$)
- Helps break relationship between output of one round and input to next round

- Thanks