16.8.20 : Recap of previous lecture

1. Encryption and decryption using classical cipher :
Vigenere, Alphabet set A, ..., Z

2. Encoding text in 5-letter alphabet A, B, C, D, E
double letters

3. Homework : To read playfair, ADFGX, Hill ciphers

Next: What do we learn from the example of Vigenere

1) Encryption and decryption can be achived with the help of a secret key exchanged bet Alice & Bob

2) Easy to encrypt and decrypt

3) If key is not available decryption is much difficult

Vigenere satisfies the first two properties of OWF (But not the third property of TOWF).

4) Frequencies of letters in English text are not observed (due to polyalphabetic nature).

5) But if the key length is found then frequncies can be identified. (Homework: Read from textbook - key length reco.)

Homework: 1) Read the method of finding key length from ciphertext of vigenere cipher

2) Using this method decrypt one of the encrypted texts given in the exercises.

<u>Modes of operating Vigenere:</u>

1. Standard mode: Repeat key

P: $p_1\ p_2\ p_3\ p_4\ p_5\ p_6\ p_7\ p_8$

K: $k_1\ k_2\ k_3\ k_1\ k_2\ k_3\ k_1\ k_2$

C $\{p_i \oplus k_i\} = p_i + k_i \bmod 26$

2. Auto key stream: (Example in 5-letter coding)

P:	E	C	C	A	B	D	D	B	
K:	C	A	B	D	C	A	B	D	(standard key repeated)
key stream:	B	C	D	D	D	D	E	E	
C:	A	E	A	D	E	A	C	A	

(key stream is used as encryption key)

3. Running key by appending text.

P :	E	C	C	A	B	D	D	B
key :	C	A	B	D				
Running key :	C	A	B	D	E	C	C	A
key stream :	A	C	D	D	A	E	E	B
C :								

Above methods of encryption make Vigenere stronger

But can they provide the third property of TDOWF?

Vernam cipher and the One Time Pad (OTP)

(Gilbert Vernam, AT & T Bell Labs 1917, patented US Telegraph office 1919. Called as Most Imp. Invention by NSA)

1. Encryption of plaintext stream $\{p_i\}$ by a key stream $\{k_i\}$ as long as text.
2. Key K is a secret information to generate key stream.
3. Ciphertext stream $\{c_i\}$ $c_i = p_i \oplus k_i$

OTP : 1) Each key stream is selected fresh for each plaintext

2) Each key stream is random.

<u>Shannon (1949)</u> : Proved that OTP had perfect secrecy.

(An unbreakable cipher)

<< Also shows that an unbreakable encryption is impossible in practice >>

If you need secure channel to exchange the key stream then why not send the plaintext itself securely ?

Practical Vernam:

1) Keystream cannot be exchanged. Only a short key K is exchanged.

2) A Pseudorandom Generator (PRG) generates the keystream sequence $\{s_i\}$ using K and an initializing vector $\underline{IV}$. $\underline{IV}$ is exchanged along with ciphertext stream $\{c_i\}$.

3) Encryption: $\{c_i\}$ $c_i := p_i \oplus s_i$

Decryption: $p_i := c_i \ominus s_i$

<u>Stream Cipher</u> : (Modern cipher, TWOF)

Set of states X subset of a field of numbers $\mathbb{F}$

State update map $\mathbb{F} : X \longrightarrow X$

Output map $f : X \longrightarrow A$ – alphabet set

Initial state $x(0) = (K, IV)$

Dynamical system

$$x(k+1) = F(x(k))$$

Output stream $\quad w(k) = f(x(k))$

Encryption $\quad c(k) = p(k) + w(k)$

TWOF property : Computation of K given $w(k)$ and IV is a difficult problem