Lecture - 01
Topic: History of Cryptography

Shifted cipher

Each letter is Shifted by k and sent. Eg- "A" is written as "A"+k (Shifted by k letters) and sent. This is easy to decode as only 26 (or 36 (if 0-9 nos are included)) possible k are there and thus its easy to check each possibility.

Rolling by wooden stick

A paper is rolled on to a stick and text is written. If seen normally, the letters would look fully shuffled, but if its rolled in the same way as it was written, it can be decoded.
eg- "MY NAME IS X" is written like

```
M              M              X
     Y     A        E     S
        N              I
```

Thus its crypted as MMXYAESNI.

Mono-Substitution cipher

We have a table where each letter is mapped to other letters and text is ciphered according to that. Here, we have here 26! ways of mapping and so its very difficult to try different possibilities.
This seems like an optimal solution, but there is a problem. In an average english text, each letter has a specific frequency of repetition.
Say letter "A" is coded to letter "K" (randomly). So frequency of letter K would be same as of the letter "A" in a normal text. So by this way, cipher text could possibly be decrypted.

Homophonic Cipher

The main problem of Mono-Substitution cipher is that, a character was substituted with only one alphabet and so the frequency didn't change.
What if its substituted with many characters to equalize the frequencies?
Say $S = \{A, B, ..Z, 0, 1, ..9, \epsilon, \alpha, \beta, \gamma, ...\}$ has usable symbols.
Say letter "A" has frequency $x\%$. We allot $\frac{x}{100} \times |S|$ number of symbols and are randomly substituted in the cipher text in place of "A". This uniforms/balences the frequency among all the symbols and hence difficult to decrypt by frequency method.
But here, storing the mapping, encrypting, and decrypting are difficult.

Vigenere's Cipher

What if we substitute "A" by any of the letters strategically? Vigenere created a table as shown below.

	A	B	C	D	..
A	B	C	D	E	..
B	C	D	E	F	..
.					
.					

A keyword is chosen and correspondingly added to the text encrypt it. Eg - Thus here, according

Actual text	M	Y	N	A	M	E	I	S	X
keyword	R	O	S	E	R	O	S	E	R
Cipher	..			F					

to the position, same letter is encrypted to different letters and thus the frequencies are balenced.
Is it a good method then?
Words like "THE", "IS", etc repeat so much in english that its very likely that it is encrypted to the same cipher text due to same relative position w.r.t keyword. Calculating the repeated strings in ciphertext and observing the distance between them will give insigts about the length of keyword. Length of keyword would be a factor of those distances and can be found out(say l). Now, characters $1, 1+l, 1+2l, ..$ are derived from same column of the table. Hence they are like monostituted and now, frequencies can be calculated out to find the keyletters and hence keyword.

Mordern Cryptography

Shannon's Cipher

$\xi = (E, D)$ is a cipher system where $E(m, k) = c$ (m is message, k is key, c is cipher text) is encyption funtion, and $D(c, k) = m$ is decryption funtion.

One Time Pad

Say m^l is a message of bits of length l, and key k^l is key of same length generated randomly.

$$E(m, k) = m^l \oplus k^l = c$$

$$
\begin{aligned}
D(c, k) &= c^l \oplus k^l \\
&= m^l \oplus k^l \oplus k^l \\
&= m^l
\end{aligned}
$$

Provided key is generated completely random, and no part of key is known to Evasdropper, they can't decrypt it as probability of c being 0 or 1 is independent of message itself. I.e,

$$Prob(cipher = c|msg = m) = Prob(cipher = c|msg = m')$$

Hence, it is safe. Disadvantages:

- key is as big as message(or more)

- key should be sent safely. Otherwise its easily decrypted.

If key length is more, either its padded at the end and xored, or key is taken till the length of message and xored.
In general, if its not a bit string, the encryption can be taken as sum modulus like:

$$E(m, k) = m^l + k^l \pmod{n} = c \text{ (if n=2, its just xor)}$$

$$
\begin{aligned}
D(c, k) &= c^l - k^l \pmod{n} \\
&= m^l + k^l - k^l \pmod{n} \\
&= m^l \pmod{n}
\end{aligned}
$$

Lecture - 03
Topic: Perfect Secrecy and Shannon's information Theory

Perfectly secrecy

OTP

For a message to be perfectly secret, the Evasdropper should not be able to get any extra information from the ciphertext. So,

$$P(M = m|C = c) = P(M = m) \quad [\text{message} = \text{m, and ciphertext} = \text{c}]$$
$$P_c(m) = P(m)$$
$$\frac{P(M = m|C = c)}{P(M = m)} = \frac{P(C = c|M = m)}{P(C = c)}$$
$$= \frac{P(C = c|M = m)}{\sum_{m' \in M} P(C = c|M = m')P(M = m')}$$

$$\left[\begin{array}{l} P(C = c|M = m') = P(K \oplus m' = c|M = m') \\ \qquad\qquad = P(K = c \oplus m'|M = m') \\ \qquad\qquad = \dfrac{1}{2^l} \quad [\text{as key is selected randomly, probability that its } c \oplus m' \text{ is } 1/2^l] \end{array} \right]$$

$$\frac{P(M = m|C = c)}{P(M = m)} = \frac{P(C = c|M = m)}{\sum_{m' \in M} P(C = c|M = m')P(M = m')}$$
$$= \frac{1/2^l}{\sum_{m' \in M} (1/2^l)P(M = m')}$$
$$= \frac{1}{\sum_{m' \in M} P(M = m')}$$
$$= \frac{1}{1}$$
$$P(M = m|C = c) = P(M = m)$$

Hence proved that it is perfectly secret.
But, what happens if key is repeated? Say a message said "Fire the gun" to a soldier which was ciphered to c using key k, though an Evasdropper technically doesn't know the key, now he would see the soldier firing after getting message and so he can guess the message. Using the ciphertext, he can get the $key = message \oplus cipher$ and if same key is used again, he would guess the message. Thus key can be used just once.
Also, if $M = m_1 =' a', m_2 =' ab'$ and,
if $c =' x', P_c(m_1) = 1$ and $P_c(m_2) = 0$ (This method reveals length of the message)
if $c =' xy', P_c(m_1) = 0$ and $P_c(m_2) = 1$.

Substitution cipher

If $M = m_1 =' aa', m_2 =' ab'$ and,
if $c =' xx'$, $P_c(m_1) = 1$ and $P_c(m_2) = 0$.
if $c =' xy'$, $P_c(m_1) = 0$ and $P_c(m_2) = 1$.
Thus its not perfectly secret.

Addition OTP

$$D(c, k) = c^l - k^l \pmod{n}$$
$$= m^l + k^l - k^l \pmod{n}$$
$$= m^l \pmod{n}$$

Proof is very similar to as OTP.

Shannon's information Theory

"No class on Friday" has more information/importance than "There is class on Friday" because having no class is a rare thing, and need to informed importantly. Having class is a regular thing and it doesn't carry much info. So,

$$\text{information} \propto \frac{1}{\text{probability of occurance}}$$
$$Info(x) \propto \frac{1}{P(x)}$$

Entropy of a message distibution(X) is defined as:

$$H(X) = -\sum_{x \in X} P(x) \log_2(P(x))$$
$$= \sum_{x \in X} P(x) \log_2(\frac{1}{P(x)})$$

Entropy is max when each of the messages has equal probability i.e, they are more uncertain. Conditonal entropy of X, given Y is:

$$H_Y(X) = \sum_{X,Y} P(x, y) \log_2(\frac{1}{P_y(x)})$$
$$= \sum_Y P(y) \sum_X P(x) \log_2(\frac{1}{P_y(x)})$$

If C is the cipher text, and if $H_C(M) \approx 0$, then its easily breakable as it is not that uncertain.