CSCI 556 : Introduction to Cryptography

Homework - 1

(1) Cryptosystem consists of keys, messages, encryption and decryption algorithms. As we know from Kerckhoff's law, security of cryptosystem is not dependent on the security or confidentiality of any of its parts but on the keys and keys only. Even Shannon reformulated the same as "Enemy already knows the system". So, it all boils down to management of the keys in the cryptosystem because we can assume that the attacker who obtains key can recover original message from encrypted data. Since key is the most important and critical part of cryptosystem, keyed cryptography is more practical nowadays.

(2) Encryption function :-

$$E(x) = ax + b \mod 26$$

Decryption function :: Inverse of cipher text

$$D(x) = c(x-b) \mod 26$$

where $c \rightarrow$ modular multiplicative inverse of a

i.e., $a * c = 1 \mod 26$

To have one-to-one mapping between plain letter and cipher letter, it is important to check a and 26 are co-prime else we can have one letter mapped to 2 different cipher letters. This basically is the concept of Affine Cipher. So, a should be relatively prime to 26. The possible values that a could be are 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 and 25. For each value of a, b can take a value from 0 to 25 inclusive. In order for E(x) to be injective, a should take one value from above defined 12 values and b should take one value from possible 26 values.

(3)

$$\Gamma = \begin{bmatrix} 7 & 14 \\ 3 & 23 \end{bmatrix}$$

$$\Gamma^{-1} = d^{-1} * adj(\Gamma)$$

d = determinant of Γ

$adj(\Gamma)$ = adjugate matrix of Γ

$$d = 7(23) - 14(3)$$

$$d = 161 - 42 = 119$$

$$dd^{-1} = 1 \bmod 26$$

$$119 * d^{-1} = 1 \bmod 26$$

$$119 * 7 = 833 = 1 \bmod 26$$

$$\Rightarrow d^{-1} = 7$$

$$adj(\Gamma) = \begin{bmatrix} 23 & -14 \\ -3 & 7 \end{bmatrix} \bmod 26 = \begin{bmatrix} 23 & 12 \\ 23 & 7 \end{bmatrix}$$

$$\Gamma^{-1} = d^{-1} * adj(\Gamma)$$

$$= 7 \begin{bmatrix} 23 & 12 \\ 23 & 7 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 161 & 84 \\ 161 & 49 \end{bmatrix} \bmod 26$$

$$\Gamma^{-1} = \begin{bmatrix} 5 & 6 \\ 5 & 23 \end{bmatrix}$$

(4)

For an $m * m$ matrix, there are 26^{m^2} possibilities.

Trying all possible $m * m$ matrixes that takes us atleast 1000 years:

$$26^{\wedge}m^2 \geq 1000 \text{ years}$$

$$26^{\wedge}m^2 \geq 1000 \times 365 \text{ days}$$

$$\geq 1000 \times 365 \times 24 \text{ hours}$$

$$\geq 1000 \times 365 \times 24 \times 60 \text{ min}$$

$$26^{\wedge}m^2 \geq 1000 \times 365 \times 24 \times 60 \times 60 \text{ seconds}$$

$$26^{m^2} \geq 1000 \times 365 \times 24 \times 60 \times 60$$

$$m^2 \log 26 \geq \log(1000 \times 365 \times 24 \times 60 \times 60)$$

$$m^2 \geq 7.4198$$

$$m \geq \sqrt{7.4198}$$

$$m \geq 2.72$$

So m has to be atleast 3 i.e., it takes more than 1000 years to try all possible $3 * 3$ matrices.

(5) I think RSA is more secure compared to matrix cipher for the following reasons :

Matrix Cipher :-

i) Vulnerable to plain-text attack : a type of attack where attacker after having access to both actual message and encrypted message just tries to encrypt plain message again & again until he finds the key.

ii) Plain text attack is not the only way. It is vulnerable to computer hacking. With the advancement of cloud technologies it only takes minutes to find the correct key.

RSA :-

i) Widely used and accepted in modern world as a very secure and effective encryption.

ii) Use of extremely large prime numbers as keys. Today these keys correspond to 617 digits.

iii) There is no known algorithm to efficiently factor such large numbers.

iv) As we know, even if public key is compromised the private key is what never leaves the sender. Message is encrypted and sent using public key which can later be decrypted by using the intended recipient's private key which is known only to the recipient.

So, RSA is more secure and effective compared to Matrix-cipher in today's world.

(6) $P(b=1) = 2/3$ $\quad P(b=0) = 1/3$

$P(r=1) = 1/2$ $\quad P(r=0) = 1/2$

$b \wedge r$ is 1 when both b and r is equal to 1. If either or both of them equals 0 then $b \wedge r$ is 0.
(r is independent of b)

(a) Probability that $c = b \wedge r$ is 1

$$P(c=1) = P(b \wedge r = 1)$$
$$= P(b=1) * P(r=1)$$
$$= 2/3 * 1/2 = 2/6 = 1/3$$

(b) Probability that $c = b \wedge r$ is 0

$$P(c=0) = P(b \wedge r = 0)$$
$$= P(b=0) * P(r=1) + P(b=1) * P(r=0) + P(b=0) * P(r=0)$$
$$= \frac{1}{3} * \frac{1}{2} + \frac{2}{3} * \frac{1}{2} + \frac{1}{3} * \frac{1}{2}$$
$$= \frac{1}{6} + \frac{2}{6} + \frac{1}{6} = 4/6 = 2/3$$

(c) As we can see from above $P(c=1) = 1/3$ and $P(c=0) = 2/3$. So, if we get to know about c then we can reveal b to some extent. For example, if $c=1$ then we for sure know $b=1$ which is a great deal of information for attacker. Hence it is not a good idea to hide b in c using the $\wedge$ operation.