CS553: Cryptography

Assignment 3: Solutions

Rohit Das (11910230)

August 18, 2019

1. CCA-Security

Formally, for any list of plaintexts $m_1, m_2, ..., m_n \in \mathcal{P}$ and ciphertexts $c_1, c_2, ..., c_n \in \mathcal{C}$ chosen by adversary, even with knowledge of corresponding ciphertexts $e_K(m_1), e_K(m_2), ..., e_K(m_n)$ and corresponding plaintexts $d_K(c_1), d_K(c_2), ..., d_K(c_n)$, it is very difficult to decrypt any ciphertext not present in the above list of ciphertexts without knowing the key.

2. Hill Cipher

2..1 Encryption

Name: ROHIT DAS. First four letters = {R,O,H,I} = {17,14,7,8} [$\because$ taking A = 0, B = 1 and so on]. Then $x = \begin{pmatrix} 17 & 14 \\ 7 & 8 \end{pmatrix}$. Given key K = $\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$,

ciphertext $y = xK = \begin{pmatrix} 17 & 14 \\ 7 & 8 \end{pmatrix} \times \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$ mod 26

$= \begin{pmatrix} 17 \times 11 + 14 \times 3 & 17 \times 8 + 14 \times 7 \\ 7 \times 11 + 8 \times 3 & 7 \times 8 + 8 \times 7 \end{pmatrix}$ mod 26 $= \begin{pmatrix} 21 & 0 \\ 23 & 8 \end{pmatrix}$ = {V,A,X,I}.

$\therefore y = e_K(x) =$ VAXI.

2..2 Inverse Key

$|K| = 11 \times 7 - 3 \times 8$ mod 26 = 53 mod 26 = 1.

Adjoint of K = $\begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix}$. $\therefore K^{-1} = \dfrac{1}{|K|} \times$ Adjoint of K $= \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix}$

2..3 Invertible?

K can be said to be invertible only if $|K| \neq 0$. Since $|K| = 53 \neq 0$, K is invertible.

2..4 Decryption

We calculated y = $\begin{pmatrix} 21 & 0 \\ 23 & 8 \end{pmatrix}$. Now, $x = d_K(y) = yK^{-1}$.

$\therefore y = \begin{pmatrix} 21 & 0 \\ 23 & 8 \end{pmatrix} \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} = \begin{pmatrix} 21 \times 7 + 0 \times (-3) & 21 \times (-8) + 0 \times 11 \\ 23 \times 7 + 8 \times (-3) & 23 \times (-8) + 8 \times 11 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} 147 & -168 \\ 137 & -96 \end{pmatrix} \bmod 26 = \begin{pmatrix} 17 & 14 \\ 7 & 8 \end{pmatrix} = \{\text{R,O,H,I}\}.$

$\therefore x = d_K(y) =$ ROHI.

3. Theorem(Perfect Secrecy): Proof

3..1 Proof 1:

Suppose the given cryptosystem provides perfect secrecy. If $\mathbf{Pr}[x_0] = 0$, for some $x_0 \in \mathcal{P}$, it trivially follows that $\mathbf{Pr}[x_0|y] = \mathbf{Pr}[x_0]$ for all $y \in \mathcal{C}$. Hence, we will only consider those plaintext elements where $\mathbf{Pr}[x_0] > 0$. Hence, it follows, using Bayes' theorem, that $\mathbf{Pr}[x|y] = \mathbf{Pr}[x]$ $\forall y \in \mathcal{C}$ is equivalent to $\mathbf{Pr}[y|x] = \mathbf{Pr}[y]$ $\forall y \in \mathcal{C}$.

Assuming $\mathbf{Pr}[y] > 0$ $\forall y \in \mathcal{C}$ ($\because$ if $\mathbf{Pr}[y] = 0$, then y is never used and can be omitted here), if we fix any $x \in \mathcal{P}$, for each $y \in \mathcal{C}$, $\mathbf{Pr}[y|x] = \mathbf{Pr}[y] > 0$. Hence, there must be at least one key K such that $e_K(x) = y$. It follows that $|\mathcal{K}| > |\mathcal{C}|$. So we have the inequalities

$$|\mathcal{C}| = |\{e_K(x) : K \in \mathcal{K}\}| \leq |\mathcal{K}|.$$

But since we are assuming $|\mathcal{C}| = |\mathcal{K}|$ [$\because$ perfect secrecy],

$$|\{e_K(x) : K \in \mathcal{K}\}| = |\mathcal{K}|.$$

This shows that there doesn't exist two keys K_1 and K_2 such that $e_{K_1}(x) = e_{K_2}(x)$. Hence, there is only one unique key K such that $e_K(x) = y$. **(Proved)**

3..2 Proof 2:

Let $n = |\mathcal{K}|$. Let $\mathcal{P} = \{x_i : 1 \le i \le n\}$ and fix a ciphertext element $y \in \mathcal{C}$. Then the keys will be $K_1, K_2, ..., K_n$ such that $e_{K_i}(x_i) = y$, $1 \le i \le n$. Using Bayes' theorem,

$$\begin{aligned}\mathbf{Pr}[x_i|y] &= \frac{\mathbf{Pr}[y|x_i]\mathbf{Pr}[x_i]}{\mathbf{Pr}[y]} \\ &= \frac{\mathbf{Pr}[\mathbf{K} = K_i]\mathbf{Pr}[x_i]}{\mathbf{Pr}[y]}\end{aligned}$$

[$\because$ probability of getting y given x_i is equal to probability of using K_i as key]

Considering perfect secrecy, $\mathbf{Pr}[x_i|y] = \mathbf{Pr}[x_i]$. From here, it follows that $\mathbf{Pr}[K_i] = \mathbf{Pr}[y]$. for $1 \le i \le n$. This says that all keys are used with equal probability $\mathbf{Pr}[y]$. But since number of keys is $|\mathcal{K}|$, we must have $\mathbf{Pr}[K_i] = \dfrac{1}{|\mathcal{K}|}$. **(Proved)**

4. Perfect Secrecy?

One-time Pad, or OTP is a one-time key used to encrypt a message in Vernam Cipher. The problem with using an OTP more than once is as follows:

Suppose our OTP is K. Let m_1, m_2 and m_3 be our messages. Then $c_1 = m_1 \oplus K$, $c_2 = m_2 \oplus K$ and $c_2 = m_3 \oplus K$. Now, if our attacker obtains even one pair of plaintext and ciphertext, the encryption is broken. Lets assume that c_2 and m_2 is obtained by attacker. Then attacker can simply XOR both of them to obtain the OTP.

$$m_2 \oplus c_2 = m_2 \oplus (m_2 \oplus K) = K.$$

Thus, this cipher becomes KPA-vulnerable if OTP is used more than once. **(Proved)**

5. Hill Vs Permutation

Permutation cipher is a special form of Hill Cipher, i.e. the permutations can be represented by a key matrix consisting of 0's and 1's, 1 representing the position of the symbol in permutation. E.g.:

Let message block size $m = 6$, and a possible key is the permutation π:

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

Thus, π(ROHITDASXXXX) = HXDXRATXOSIX.

This can be represented by a 6×6 key matrix K:

$$K = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \text{,i.e. } k_{i,j} = \begin{cases} 1 \text{ if } j = \pi(i) \\ 0 \text{ otherwise} \end{cases}$$

Encryption of message $m =$ ROHITDASXXXX (18,15,8,9,20,4,1,19,24,24,24,24):

$$x = \begin{pmatrix} R & O & H & I & T & D \\ A & S & X & X & X & X \end{pmatrix} = \begin{pmatrix} 18 & 15 & 8 & 9 & 20 & 4 \\ 1 & 19 & 24 & 24 & 24 & 24 \end{pmatrix}$$

$$\text{cipher text } y = xK = \begin{pmatrix} 18 & 15 & 8 & 9 & 20 & 4 \\ 1 & 19 & 24 & 24 & 24 & 24 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 8 & 4 & 18 & 20 & 15 & 9 \\ 24 & 24 & 1 & 24 & 19 & 24 \end{pmatrix} = \begin{pmatrix} H & D & R & T & O & I \\ X & X & A & X & S & X \end{pmatrix} = \text{HXDXRATXOSIX.}$$