[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2022-2023
Scribed by: Rathva Kaushikkumar Sanjaybhai (202051156) — Week : 1 (2nd lecture #)

1 One way function

Using one way funtion we can easily findout the output from input. But doing the otherway arround is computationaly difficult task.

Example : For given two large prime numbers multiplication is a oneway function. We can easily calculate answer to multiplication of amy two numbers in polinomial time. But calculting back the prime numbers from the ouput.We have to facturize it in prime numbers to do that and it's computationally intensive task.

2 Substitution box :

It's a function from $A \to B$ where $|B| \leq |A|$

example :
$S1 : \{1, 2, 3, 4\} \to \{1, 2, 3\}$

$S1(1) = 1$, $S1(2) = 3$, $S1(3) = 2$, $S1(1) = 4$

3 Transposition Cipher :

This is a function which is mapped from domain to co-domain.

Example : $M = m_1\ m_2\ m_3\ .\ .\ .\ m_t$
Here, M is plain text.
e : permutation on t elements $\to$ Secret key.

Encryption : $C = m_{e(1)}\ m_{e(2)}\ m_{e(3)}\ .\ .\ .m_{e(t)}$
Here, C is cipher text.

Decryption : $n = C_{e^{-1}(1)}\ C_{e^{-1}(2)}\ C_{e^{-1}(3)}\ .\ .\ .\ C_{e^{-1}(t)}$
Here, n is the plain text that is decrypted from cipher text.

4 Permutation :

Example :
C A E S A R = $m_1\ m_2\ m_3\ ...\ m_6$

$$e\ :\{ \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 3 & 5 & 2 \end{matrix} \}_{Encryption}$$

Cipher text = R S C E A A = $C_1\ C_2\ C_3\ ...\ C_6$

$$d = e^{-1} : \{ \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 2 & 5 & 1 \end{matrix} \}_{Decryption}$$

Plain text : C A E S A R

5 Substitution Cipher :

M = $m_1\ m_2\ m_3\ ...\ m_t$
A = $a, b, c, d, ..., z\ M_i\ \epsilon$ A

e : substitution from A to A.
e $\rightarrow$ secret key.

ex. e(a) = z , e(b) = d , e(c) = a
a b c $\rightarrow$ plain text
z d a $\rightarrow$ cipher text

6 Affine cipher :

$A \rightarrow 0$
$B \rightarrow 1$
$C \rightarrow 2$
.
.
.
$Z \rightarrow 25$

6.1 Encryption function:

$C\ =\ e(x, k)\ =\ (ax + b) mod\ 26\ = c$
where, $a, b, c\ \epsilon\ Z_{26}$

6.2 Decryption function:

$X\ =\ d(c, k)\ =\ ((c - b)a^{-1}) mod\ 26\ = c$

6.3 Exapmple :

$Z_6 = 0, 1, 2, 3, 4, 5 \quad x, y \epsilon Z_6$

$+ \ mod\ 6 \ : \ +_6 \rightarrow \ Z = (x + y)$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$0 \neq x \ \epsilon \ Z_6$
if $gcd(x, 6) = 1$
then y such that
$x *_6 y \ = \ 1$

for m and (xy - 1)
$xy \ - \ 1 \ = \ tm$
$1 \ = \ t_1 m \ + \ xy \quad t_1 \ = \ (-t)$

gcd(x,m) = ax + bm

Example : m=7,x=3

extended euclidion algo.

$1 = am + yz$
$1 = 3 - (1X2)$
$= 3 + (-1X2)$
$= 3 + (-1)17 + 5X3$
$= 6X3 + (-1)X17$

$so, y = 6, x = 3, t = 1, m = 17.$

$*_6 \ : \ (x * y) = Z$

$*_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$0 \neq x \ \epsilon \ Z_m$
if $gcd(x, m) = 1$
then y such that
$x *_m y \ = \ 1$

7 Playfair cipher :

secret key = playfair example
Here we are taking 5x5 matrix so we only have 25 distinct alphabets.So we are taking I=J.
Steps

1. Make a 5x5 matrix and add alphabets of secret key such that alphabets don't repeat.

$$\begin{matrix} P & L & A & Y & F \\ I & R & E & X & M \\ - & - & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \end{matrix}$$

2. Fill all the remaining alphabets in lexicographical order such that they don't repeat.

$$\begin{array}{ccccc} \hline |\,P & L & A & Y & F\,| \\ |\,I & R & E & X & M\,| \\ \hline B & C & D & G & H \\ K & N & O & Q & S \\ T & U & V & W & Z \end{array}$$

Here we have taken plain text HIDE.

3. Break text into groups of 2 alphabets and if their are odd no of letters append z at the end.
4. Now for the group mark both letters on the table and replace them with letters in same row relatively of the rectangle made by the group's letters.
5. If both letters are in same row/column replace them with next element in circular meaner.

For plain text HIDE $\rightarrow$ HI DE
HI DE
$\downarrow$ $\downarrow$
BM OD