**Cryptology** 4th August, 2015

# Lecture 1: Introduction to Cryptology

*Instructor: Dr. Goutam Paul* *Scribe: Laltu Sardar*

## 1 Introduction

The word "Crypto" came from Greek word "$\kappa\rho\upsilon\pi\tau o\zeta$( krypts)" which means "hidden or secret"; and the word "Graphy" came from "$\gamma\rho\alpha\phi\epsilon\iota\nu$ (graphein)" which means "writing". That is Cryptography is art of secure writing. Crypto was first needed in ancient days when sending message from one place to others secretly became necessary. Now the time has been changed and crypto has been spread out in a lot of places.

### 1.1 Goals of Cryptography

In essence, cryptography concerns four main goals:

1. Privacy/Confidentiality
2. Integrity/ Message Authentication
3. Authentication/ Identification
4. Non-Repudiation

#### 1.1.1 Privacy/Confidentiality

Privacy or message confidentiality tells that only an authorized recipient should be able to extract the contents of the message from its encrypted form. It guarantees the protection of transmitted data from passive attacks. Resulting from steps to hide, stop or delay free access to the encrypted information.

#### 1.1.2 Integrity / Message Authentication

Message integrity ensures that the information has not been altered by unauthorized or unknown means. One must have the ability to detect data manipulation or change by unauthorized parties.

#### 1.1.3 Authentication/ Identification

Authentication i.e. sender authentication ensures that the recipient should be able to verify from the message, the identity of the sender, the origin or the path it travelled (or combinations) so to validate claims from emitter or to validated the recipient expectations.

### 1.1.4 Non-Repudiation

Non-repudiation prevents either sender or receiver from denying a message. Thus, when a message is sent, the receiver can prove that the message was in fact send by the alleged sender. Similarly, when a message is received, the sender can prove the alleged receiver in fact received that message.

In respect to the above goals there are solutions like Message Encryption, Authentication Code, Identification Schema and Commitment Scheme respectively.

# 2 Cryptosystem

**Definition 2.1** *A cryptosystem $S = (P, C, K, E, D)$ is five tuple where*

$P$ = *Plaintext Space (finite set of all possible messages),*
$C$ = *Ciphertext Space (finite set of all possible encrypted messages),*
$K$ = *Keyspace(finite set of all possible keys),*
$E$ = $\{e_k : P \to C, k \in K\}$ *is the family of decryption functions,*
$D$ = $\{d_k : P \to C, k \in K\}$ *is the family of decryption functions and* $\forall x \in P, d_k(e_k(x)) = x$.

## 2.1 Examples of Ciphers:

Let us start with some classical examples of cryptographic schemes in which both the sender and the receiver agree upon a common key secretly before the actual communication starts.

### 2.1.1 Caesar Cipher:

This cryptographic scheme was discovered by Julius Caesar, used around 2000 years ago, during war, To keep the messages secrete form the enemies or the messenger Julius Caesar introduced a new method. Before going to the war front Julius Caesar and his generals agreed upon a secret number, say 3, which is the key of the cryptosystem. When Julius Caesar needed to send messages to the generals at the war front, he just cyclically shifted every letter of the command or instruction by 3 positions to the right.

For example If we take the English upper case alphabets, we have altogether 26 letters. So if we shift cyclically each letter of the English alphabets 3 times to the right, A will be shifted to D, B will be shifted to E,..., X will be shifted to A, Y will be shifted to B and finally, Z will be shifted to C.

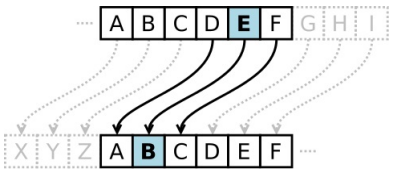


Figure 1: Caesar Cipher with English alphabet with key k=3

Thus in his cryptosystem

$$
\begin{aligned}
&P = \{0, 1, \ldots, 25\} \\
&C = P \\
&K = \{\}/\{3\} \\
&E = \{e : P \to C, \text{ where } e(x) = x + 3 \bmod (26), \forall x \in P\}, \\
&D = \{d : C \to P, \text{ where } d(y) = y - 3 \bmod (26), \forall y \in C\}
\end{aligned}
$$

Now if we assume that an adversary only has a piece of cipher text along with the knowledge that this cipher text is obtained by using shift cipher then, if the adversary tries try every 26 keys and he can see which key decrypts the cipher text into a plain text.

### 2.1.2 Shift Cipher:

Shift cipher is just a generalization of Caesar cipher. The only difference is that here key is not fixed. So keyspace contains all $0, 1, \ldots, 25$ elements. In this cryptosystem:

$$
\begin{aligned}
P &= \{0, 1, \ldots, 25\} \\
C &= P \\
K &= \{0, 1, ..., 25\} \\
E &= \{e_k : P \to C, k \in K \text{ where } e_k(x) = x + k \bmod (26), \forall x \in P\}, \\
D &= \{d_k : C \to P, k \in K \text{ where } d_k(y) = y - k \bmod (26), \forall y \in C\}
\end{aligned}
$$

Here also if adversary tries only 26 keys then encrypted message can be decrypted.

### 2.1.3 Affine Cipher:

Thus looking at the weaknesses of previous cryptosystems it is obvious to have more strong cryptosystems. Affine Cipher is just one step ahead to shift cipher. In this cryptosystem:

$$
\begin{aligned}
P &= \{0, 1, \ldots, 25\} \\
C &= P \\
K &= \{(a, b) : a, b \in Z_{26}\} \\
E &= \{e_k : P \to C, e_k(x) = ax + b, \forall x \in P, \text{ where } k = (a, b) \in (Z_{26} \times Z_{26})\} \\
E &= \{d_k : C \to P, d_k(y) = \frac{y - b}{a}, \forall y \in C, \text{ where } k = (a, b) \in (Z_{26} \times Z_{26})\}
\end{aligned}
$$

Since in this cryptosystem size of the keyspace is $26^2$ adversary has to give more effort to decrypt ciphertext.

It can seen here in decryption function dividing by a just not a normal division but a modular division. So for any value of $a \in Z_{26}$, $a^{-1}$ may not exist. For example for $a = 4$,

$a^{-1}$ mod (26) does not exists. So there may be question that when inverse exists. For this let's go through the followings.

## 2.2 Extended Euclidean Algorithm

Let $x, y \in Z$ and we are to find $gcd(x, y)$. Let $r_0 = x$ and $r_1 = y$. Then by Euclidean Algorithm and successively applying the division algorithm, we have

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2, 0 < r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3, 0 < r_3 < r_2 \\
&\dots \\
r_{j-2} &= r_{j-1} q_{j-1} + r_j, 0 < r_j < r_{j-1} \\
&\dots \\
r_{n-3} &= r_{n-2} q_{n-2} + r_{n-1}, 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_n + 0
\end{aligned}$$

Then $r_n = gcd(x, y)$.

**Correctness:** From the above equations if we go down to upward we will see $r_n \mid r_{n-1}$, $r_n \mid r_{n-2}, \dots, r_n \mid r_0$ and $r_n \mid r_1$. So $r_n$ is a common divisor of both x and y.

Let $gcd(x, y) = h$. Then we must have $r_n \leq h$.Now if we go up to downward we will see $h \mid r_2$, $h \mid r_3, \dots, h \mid r_n$. So $h \leq r_n$. Thus $h = r_n$. So $r_n = gcd(x, y)$.