GLIMPSES OF CRYPTOGRAPHY

MD Karimulla Haque

Introduction

- We need information to share/express our ideas
- Some information are valuable. Hence we need protection
- One of protection method is Cryptography
- Cryptography is used in ATM, Email-Password, E-Payment, E-Commerce, Electronic Voting, Defense Services, Securing Data, Access Control etc.

What is Cryptography?

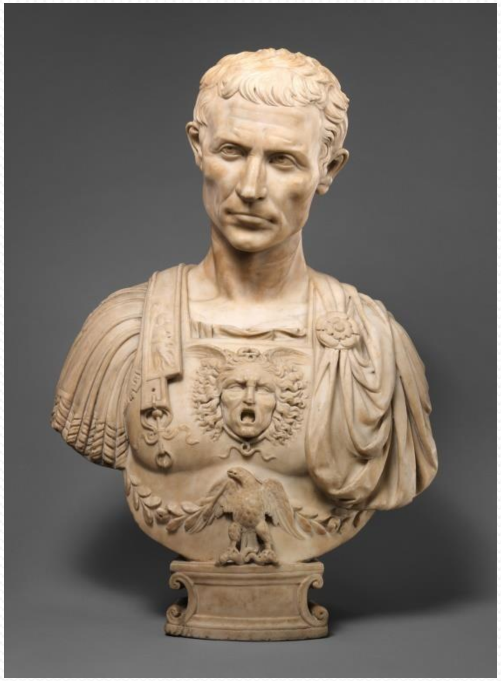
- Cryptography is the practice and study of hiding information
- It is a branch of both Mathematics and Computer science

Basic Terminology

- Plaintext – original message
- Ciphertext – coded message
- Encipher (Encrypt) – converting Plaintext to Ciphertext
- Decipher (Decrypt) – reconverting Ciphertext to Plaintext
- Cipher – algorithm for performing Encryption or Decryption
- Key – unique info used in cipher known only sender and receiver

Caesar cipher

- One of the earliest known example of substitution cipher
- Said to have been used by Julius Caesar to communicate with his army (secretly)
- Each character of a plaintext message is replaced by *n* position down in the alphabet



Example

- First row denotes the plaintext
- Second row denotes the ciphertext
- Ciphertext is obtain by shifting the original letter by *n* position to the right
- In this example, it is shifted by 3 to the right
  - A becomes D
  - B becomes E
  - X becomes A and so on…

A	B	C	D	E	…	…	X	Y	Z
D	E	F	G	H	…	…	A	B	C

- Suppose the following plaintext is to be encrypted

ATTACK AT DAWN

- By shifting each letter by 3 to the right.
- The resulting ciphertext would be

DWWDFN DW GDZQ

A	B	C	D	E	...	...	X	Y	Z
D	E	F	G	H	...	...	A	B	C

- One could shift other than 3 letters apart
- The offset (Number of shift) is called key
- Decryption process
  - Given that the key is known, just shift back *n* letter to the left
- Example:
  - Ciphertext:

WJYZWS YT GFXJ

  - Key used 5
  - Plaintext:

RETURN TO BASE

A	B	C	D	E	…	…	X	Y	Z
V	W	X	Y	Z	…	…	S	T	U

Math behind this

- Can be represented using modular arithmetic
- Assume that:
  - A= 0, B= 1, C= 2, …, Y= 24, Z= 25
- Encryption process can be represented as:

$$E(x) = (x + k) \ (mod\ 26)$$

- Where
  - x is the plaintext
  - k is the number of shift
  - There are 26 letters in the alphabet (English alphabet)

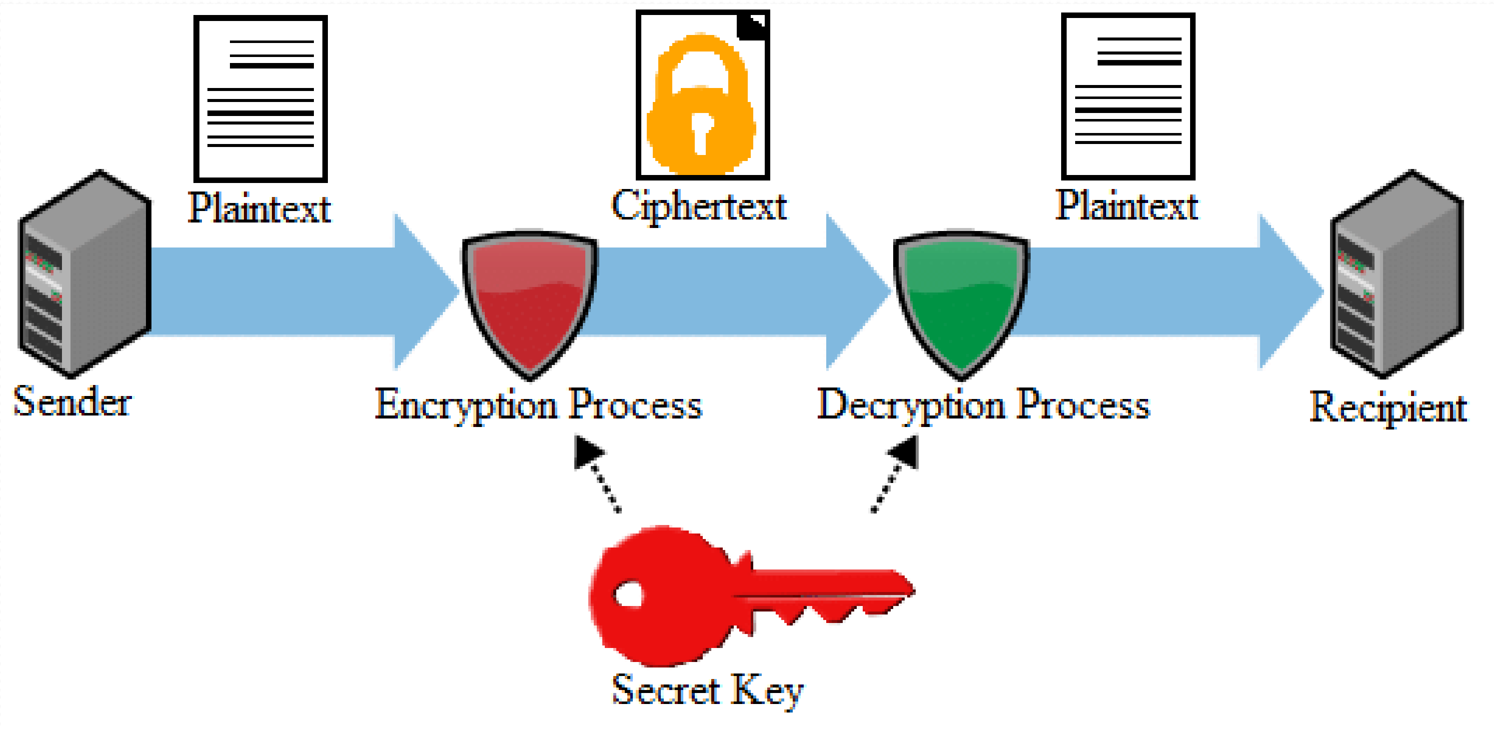
Math behind this

- Can be represented using modular arithmetic
- Assume that:
  - A= 0, B= 1, C= 2, …, Y= 24, Z= 25
- Decryption process can be represented as:

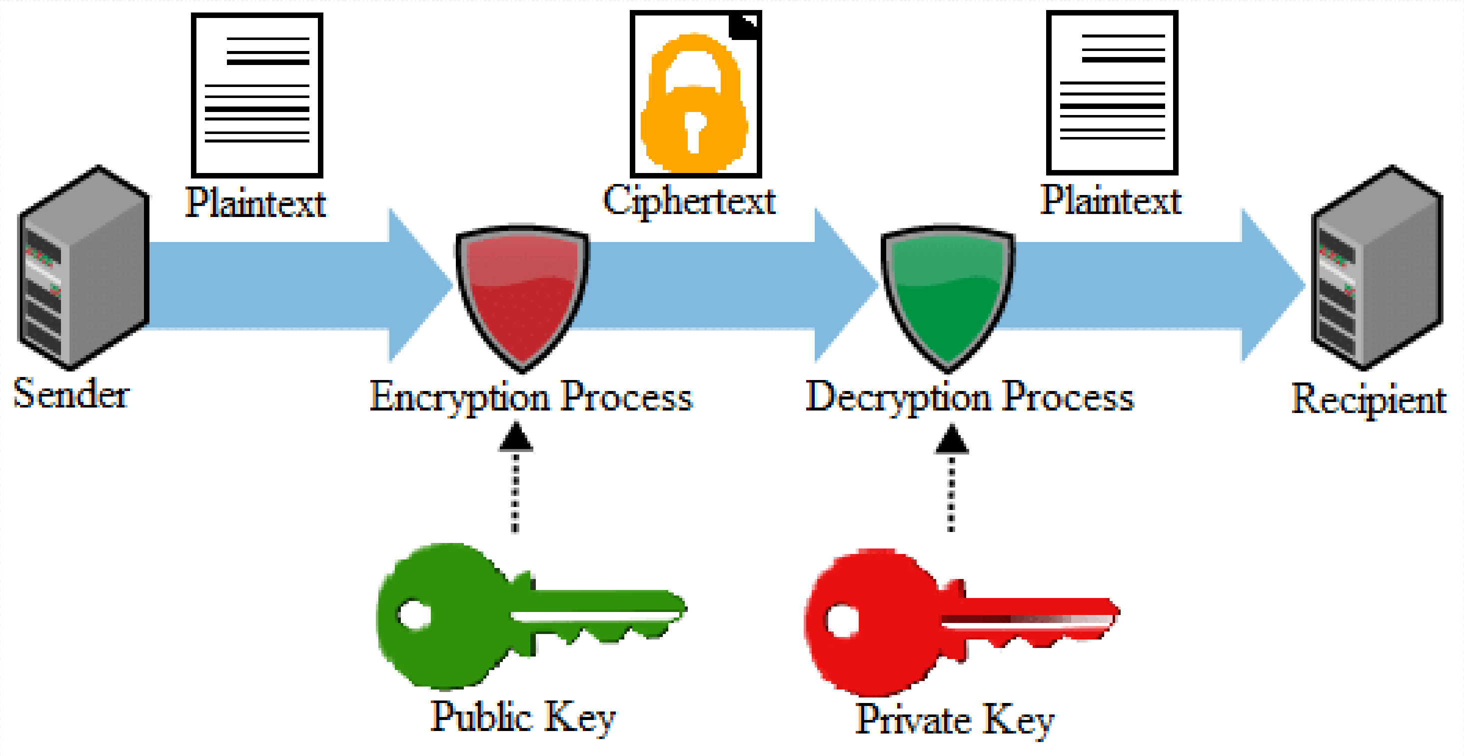
$$D(y) = (y - k)\ (mod\ 26)$$

- Where
  - y is the ciphertext
  - k is the number of shift
  - There are 26 letters in the alphabet (English alphabet)

Symmetric Ciphers



Asymmetric Ciphers

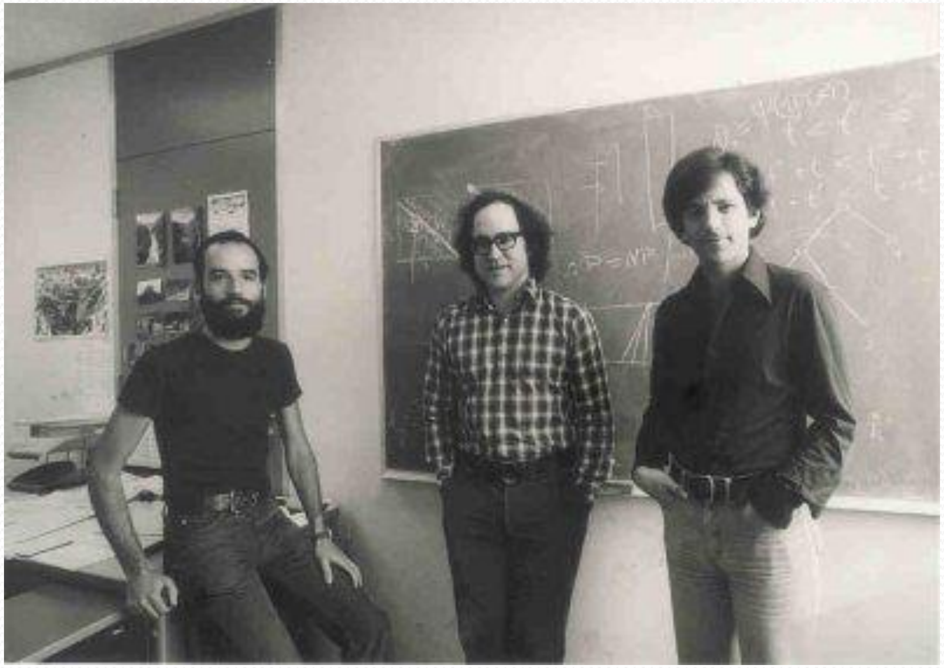


RSA

- The most common public-key algorithm is the RSA cryptography, named for its inventors (Rivest, Shamir and Adleman)
- RSA do – Encryption/Decryption/Key Generation
- Two types of keys
  - Private key (to be kept confidential)
  - Public key (known to everyone)

Inventers of RSA

- Ronald L. **R**ivest, Adi **S**hamir and Leonard **A**dleman



Choosing keys

- Choose two large prime numbers p, q (e.g., 1024 bits each)
- Compute $n = pq$
- $Z_n{}' = Z_{pq}{}'$ contains all integers in the range $[1, pq)$ that are relatively prime to both p and q
- Size of $Z_n{}'$ is $\emptyset(pq) = (p-1)(q-1) = z$ (say)
- Choose e (with $1 < e < z$) that has no common factors with z (i.e., e and z are relatively prime ; $\gcd(e, z) = 1$)
- Choose d such that $ed - 1$ is exactly divisible by z (i.e., $ed \; mod \; z = 1$; $ed = 1 + kz$, k is an integer)
- Public key is (n, e)
- Private key is d

Encryption

- To encrypt plaintext,
- a given message M, where $M \in \mathbb{Z}_n - \{0\}, 0 < M < n$
- Compute $C = M^e \ mod \ n$
  - (i.e., remainder when M^e is divided by n)

Decryption

- To decrypt received ciphertext,
- a given ciphertext C, where $C \in \mathbb{Z}_n - \{0\}$
- compute $M = C^d \bmod n$
  - (i.e., remainder when C^d is divided by n)

Example

- Receiver chooses $p = 5, q = 7$. Then $n = 35, z = 24$
- $e = 5$ (so that e and z are relatively prime)
- $d = 29$ (so that $ed - 1$ exactly divisible by z)

	letter	m	m^e	$c = m^e \; mod \; n$
encrypt:	I	12	1524832	17

	c	c^d	$m = c^d \; mod \; n$	letter
decrypt:	17	481968572106750915091411825223071697	12	I

RSA recommendation

- The number of bits for n should be at least 1024. This means that n should be around 2^{1024} or, 309 decimal digits.
- The two primes p and q must each be at least 512 bits
- The values of p and q should not be very close to each other.
- Both p-1 and q-1 should have at least one large prime factor.
- The ratio p/q should not be close to a rational number with a small enumerator and denominator.
- The modulus n must not be shared.

RSA numbers

- RSA-260 has 260 decimal digits (862 bits) has not been factored so far
- RSA-2048 has 617 decimal digits (2048 bits). It is the largest of the RSA numbers and carried the largest cash prize for its factorization, $200,000

References

- Cryptanalytic Attacks on RSA by Song Y. Yan
- Introduction toCryptography by Hans Delfs & Helmut Knebl
- Cryptography Theory and Practice by Douglas R. Stinson
- Pictures were taken from Google Images.

Thank You

- **Any query…?**
- **Email:** *mdkarimullahaque@gmail.com*