Glimpses of Cryptography

MAC MATH FEST 2021

MD Karimulla Haque

Guided by,
Dr. Nanda Das

June 27, 2021

- We need information to share/express our ideas.

Introduction

- We need information to share/express our ideas.
- Some information are valuable. Hence we need protection.

Introduction

- We need information to share/express our ideas.
- Some information are valuable. Hence we need protection.
- One of protection method is Cryptography.

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.

What is Cryptography?

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

- **Plaintext:** original message

Basic Terminology

- **Plaintext:** original message
- **Ciphertext:** coded message

Basic Terminology

- **Plaintext:** original message
- **Ciphertext:** coded message
- Encipher (**Encrypt**): converting Plaintext to Ciphertext.

Basic Terminology

- **Plaintext:** original message
- **Ciphertext:** coded message
- Encipher (**Encrypt**): converting Plaintext to Ciphertext.
- Decipher (**Decrypt**): reconverting Ciphertext to Plaintext.

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.

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.

- One of the earliest known example of **substitution cipher.**

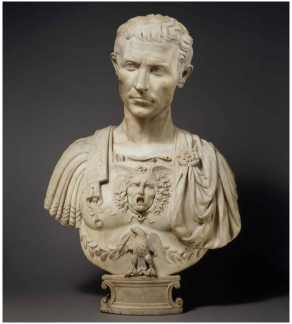


Figure: Julius Caesar

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**).

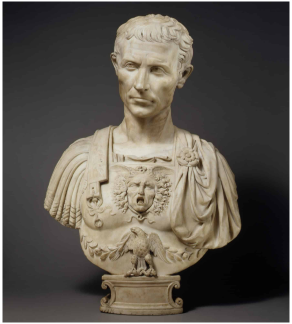


Figure: Julius Caesar

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.

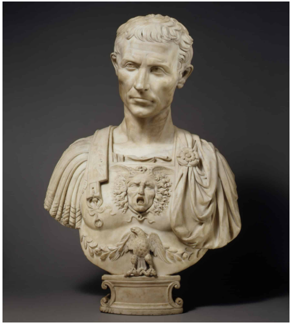


Figure: Julius Caesar

- First row denotes the plaintext.

Figure: The earliest cipher equipment developed for substitution ciphers.

Example

- First row denotes the plaintext.
- Second row denotes the ciphertext.

Figure: The earliest cipher equipment developed for substitution ciphers.

- First row denotes the plaintext.
- Second row denotes the ciphertext.
- Ciphertext is obtain by shifting the original letter by n position to the right.

Figure: The earliest cipher equipment developed for substitution ciphers.

- 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 $\cdots$

A	B	C	$\cdots$	X	Y	Z
D	E	F	$\cdots$	A	B	C

Figure: The earliest cipher equipment developed for substitution ciphers.

Continue...

- Suppose the following plaintext is to be encrypted

ATTACK AT DAWN

Continue...

- 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	$\cdots$	X	Y	Z
D	E	F	$\cdots$	A	B	C

Continue...

- One could shift other than 3 letters apart.

Continue...

- One could shift other than 3 letters apart.
- The offset (**Number of shift**) is called **key**.

Continue...

- 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.

- 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	...	X	Y	Z
V	W	X	...	S	T	U

Math behind this

- Can be represented using modular arithmetic.

Math behind this

- Can be represented using modular arithmetic.
- Assume that:
  - $A = 0, B = 1, C = 2, \dots, Y = 24, Z = 25$

Math behind this

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

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

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

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

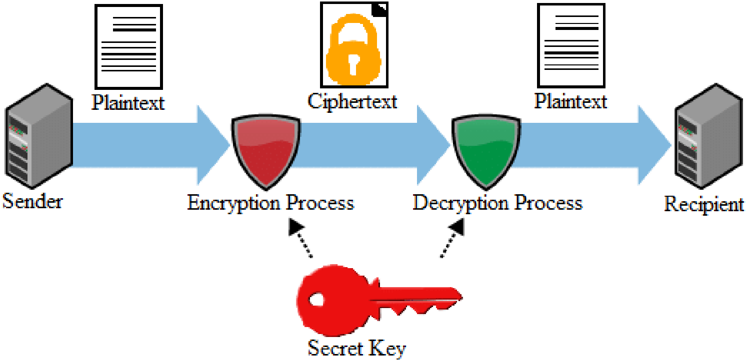
- Decryption process can be represented as:

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

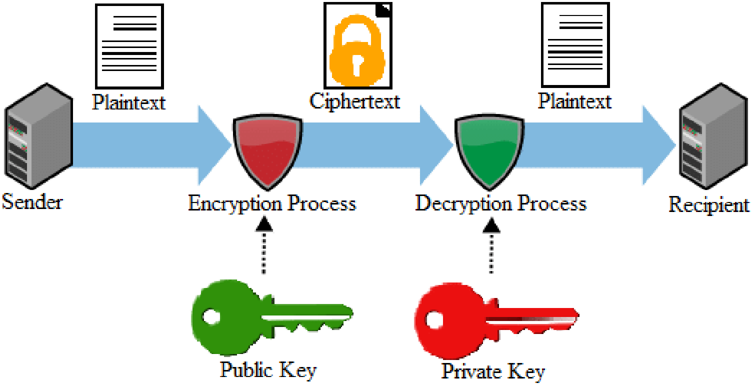
where

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

Symmetric Ciphers



Asymmetric Ciphers



- The most common public-key algorithm is the RSA cryptography, named for its inventors (**R**ivest, **S**hamir and **A**dleman) .

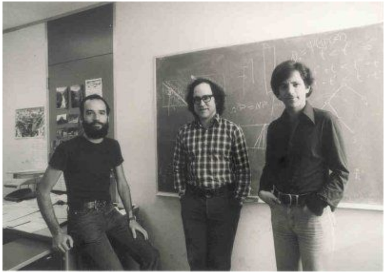


Figure: Inventers of RSA (Ronald L. **R**ivest, Adi **S**hamir and Leonard **A**dleman)

- The most common public-key algorithm is the RSA cryptography, named for its inventors (**R**ivest, **S**hamir and **A**dleman) .
- RSA do – Encryption/Decryption/Key Generation .

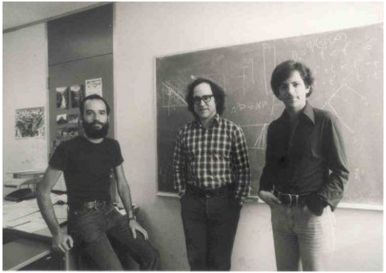


Figure: Inventers of RSA (Ronald L. **R**ivest, Adi **S**hamir and Leonard **A**dleman)

- The most common public-key algorithm is the RSA cryptography, named for its inventors (**R**ivest, **S**hamir and **A**dleman) .
- RSA do – Encryption/Decryption/Key Generation .
- Two types of keys

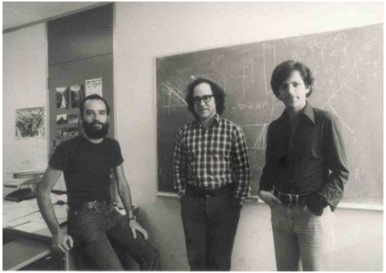


Figure: Inventers of RSA (Ronald L. **R**ivest, Adi **S**hamir and Leonard **A**dleman)

RSA

- The most common public-key algorithm is the RSA cryptography, named for its inventors (**R**ivest, **S**hamir and **A**dleman) .
- RSA do – Encryption/Decryption/Key Generation .
- Two types of keys
  - Private key (to be kept confidential)

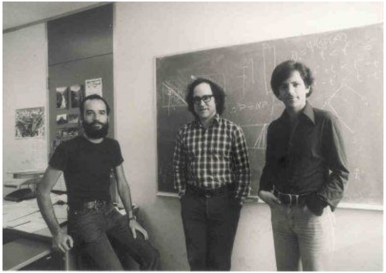


Figure: Inventers of RSA (Ronald L. **R**ivest, Adi **S**hamir and Leonard **A**dleman)

- The most common public-key algorithm is the RSA cryptography, named for its inventors (**R**ivest, **S**hamir and **A**dleman) .
- RSA do – Encryption/Decryption/Key Generation .
- Two types of keys
  - Private key (to be kept confidential)
  - Public key (known to everyone)

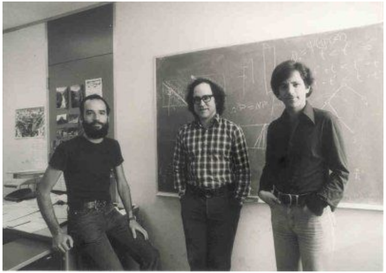


Figure: Inventers of RSA (Ronald L. **R**ivest, Adi **S**hamir and Leonard **A**dleman)

Choosing keys

- Choose two large prime numbers p, q (e.g., 1024 bits each)

Choosing keys

- Choose two large prime numbers p, q (e.g., 1024 bits each)
- Compute $\boldsymbol{n = pq}$

Choosing keys

- Choose two large prime numbers p, q (e.g., 1024 bits each)
- Compute $\boldsymbol{n = pq}$
- $Z_n{}' = Z_{pq}{}'$ contains all integers in the range $[1, pq)$ that are relatively prime to both p and q

Choosing keys

- Choose two large prime numbers p, q (e.g., 1024 bits each)
- Compute $\boldsymbol{n = pq}$
- $Z_n{'} = Z_{pq}{'}$ contains all integers in the range $[1, pq)$ that are relatively prime to both p and q
- Size of $Z_n{'}$ is $\phi(pq) = \boldsymbol{(p-1)(q-1) = z}$ (say)

Choosing keys

- Choose two large prime numbers p, q (e.g., 1024 bits each)
- Compute $\boldsymbol{n = pq}$
- $Z_n{}' = Z_{pq}{}'$ contains all integers in the range $[1, pq)$ that are relatively prime to both p and q
- Size of $Z_n{}'$ is $\phi(pq) = \boldsymbol{(p-1)(q-1) = z}$ (say)
- Choose $\boldsymbol{e}$ (with $1 < e < z$) that has no common factors with z (i.e., e and z are relatively prime; $\mathbf{gcd}(\boldsymbol{e}, \boldsymbol{z}) = \mathbf{1}$)

Choosing keys

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

Choosing keys

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

Choosing keys

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

- To encrypt plaintext,

- To encrypt plaintext,
- a given message M, where $M \in \mathbb{Z}_n - \{0\}$, $0 < M < n$

Encryption

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

Decryption

- To decrypt received ciphertext,

- To decrypt received ciphertext,
- a given message C, where $C \in \mathbb{Z}_n - \{0\}$

Decryption

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

Example

- Receiver choose $p = 5, q = 7$. Then $n = 35, z = 24$

Example

- Receiver choose $p = 5, q = 7$. Then $n = 35, z = 24$
- $e = 5$ (so that e and z are relatively prime)

Example

- Receiver choose $p = 5, q = 7$. Then $n = 35, z = 24$
- $e = 5$ (so that e and z are relatively prime)
- $d = 29$ (so that $ed1$ exactly divisible by z)

Example

- Receiver choose $p = 5, q = 7$. Then $n = 35, z = 24$
- $e = 5$ (so that e and z are relatively prime)
- $d = 29$ (so that $ed1$ exactly divisible by z)
- **encrypt**:

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

- Receiver choose $p = 5, q = 7$. Then $n = 35, z = 24$
- $e = 5$ (so that e and z are relatively prime)
- $d = 29$ (so that $ed1$ exactly divisible by z)
- **encrypt**:

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

- **decrypt**:

c	c^d	$m = c^d \mod n$	letter
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.

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**.

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.

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.

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 $\frac{p}{q}$ should not be close to a rational number with a small enumerator and denominator.

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 $\frac{p}{q}$ should not be close to a rational number with a small enumerator and denominator.
- The modulus n must not be shared.

RSA Numbers

- RSA numbers are a collection of large semiprimes published by RSA Laboratories to encourage research in integer factorization.

RSA Numbers

- RSA numbers are a collection of large semiprimes published by RSA Laboratories to encourage research in integer factorization.
- RSA-768 (with 768 bits, 232 decimal digits) was factored in December 2009 after about 2,000 core-years of computation.

RSA Numbers

- RSA numbers are a collection of large semiprimes published by RSA Laboratories to encourage research in integer factorization.
- RSA-768 (with 768 bits, 232 decimal digits) was factored in December 2009 after about 2,000 core-years of computation.
- RSA-1024 (with 1024 bits, 309 decimal digits) remains unbroken and is still considered secure for many applications.

RSA Numbers

- RSA numbers are a collection of large semiprimes published by RSA Laboratories to encourage research in integer factorization.
- RSA-768 (with 768 bits, 232 decimal digits) was factored in December 2009 after about 2,000 core-years of computation.
- RSA-1024 (with 1024 bits, 309 decimal digits) remains unbroken and is still considered secure for many applications.
- 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.

RSA Numbers

- RSA numbers are a collection of large semiprimes published by RSA Laboratories to encourage research in integer factorization.
- RSA-768 (with 768 bits, 232 decimal digits) was factored in December 2009 after about 2,000 core-years of computation.
- RSA-1024 (with 1024 bits, 309 decimal digits) remains unbroken and is still considered secure for many applications.
- 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.
- As of today, no RSA number larger than 768 bits has been successfully factored, highlighting the strength of modern public-key cryptography.

References

- Yan, S. Y. Cryptanalytic Attacks on RSA. Springer, 2008.
- Delfs, H. and Knebl, H. Introduction to Cryptography: Principles and Applications. Springer, 3rd Edition, 2015.
- Stinson, D. R. Cryptography: Theory and Practice. Chapman Hall/CRC, 4th Edition, 2018.
- Lecture video (Bengali) is available at: `https://youtu.be/XRfuKKCQVBA?t=1460`
- Pictures were taken from Google Images.

Thank You