Introduction to Public-Key Cryptography

Sabyasachi Karati

Assistant Professor
School of Computer Sciences
National Institute of Science Education and Research (NISER), HBNI
Bhubaneswar, India

Outline for section 1

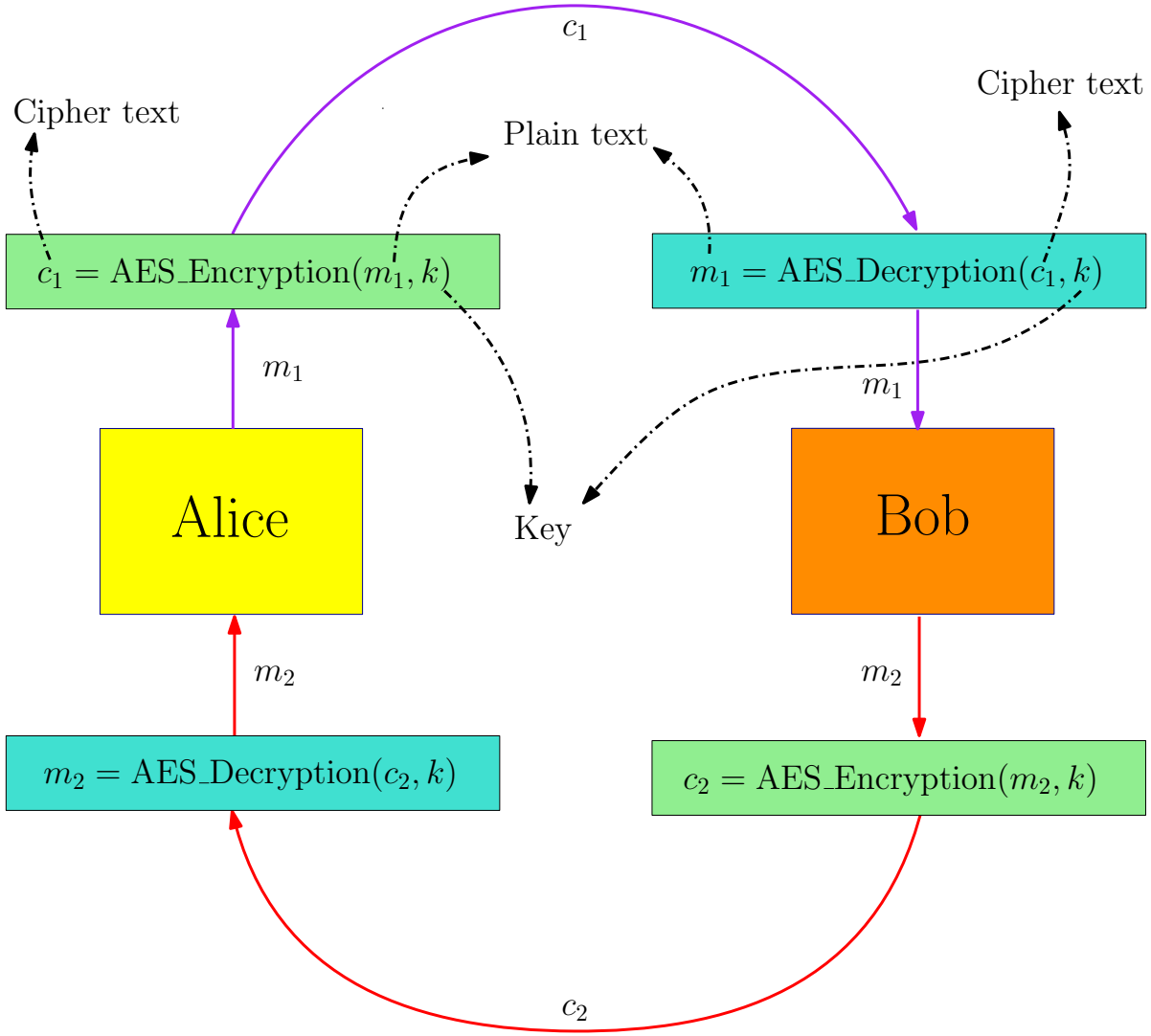
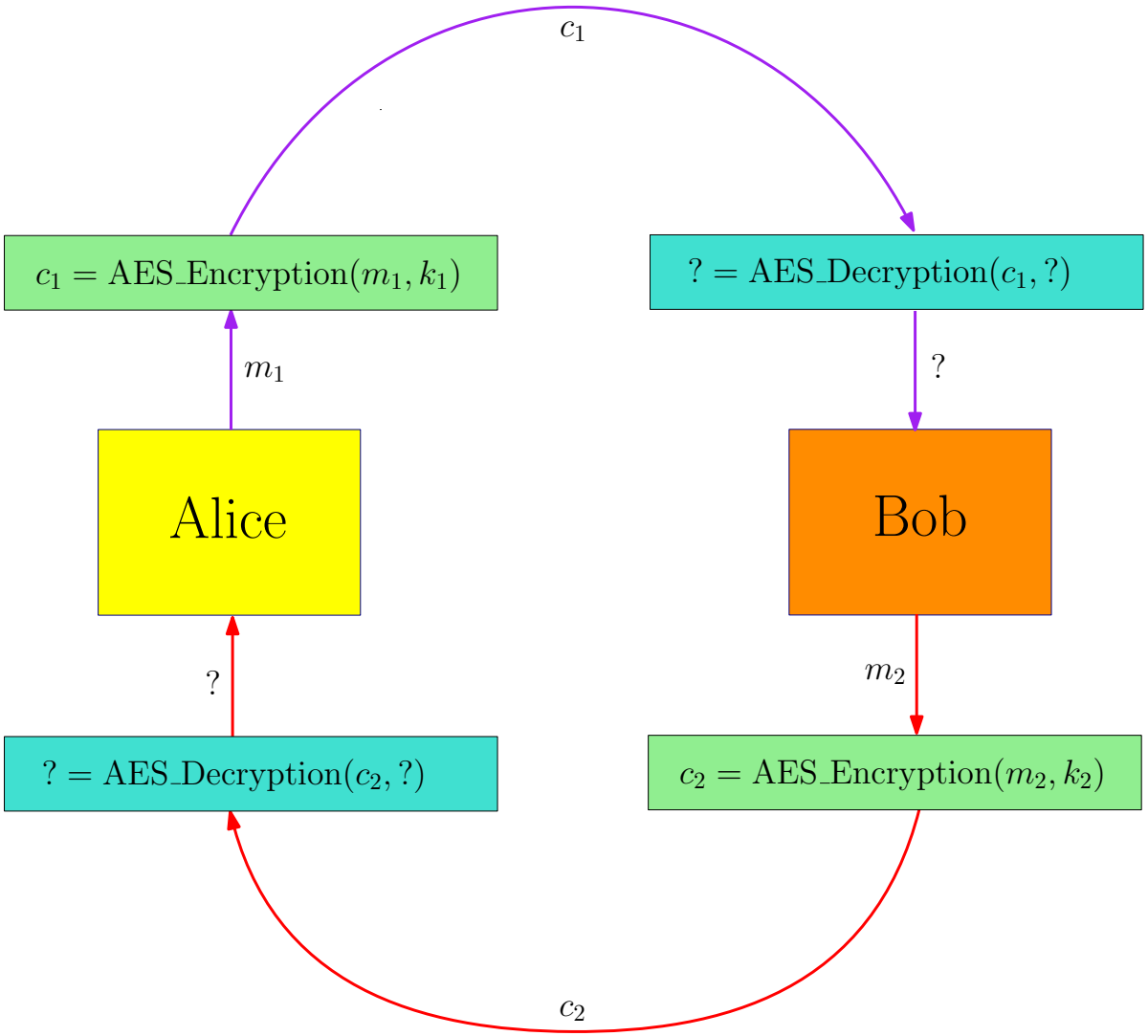
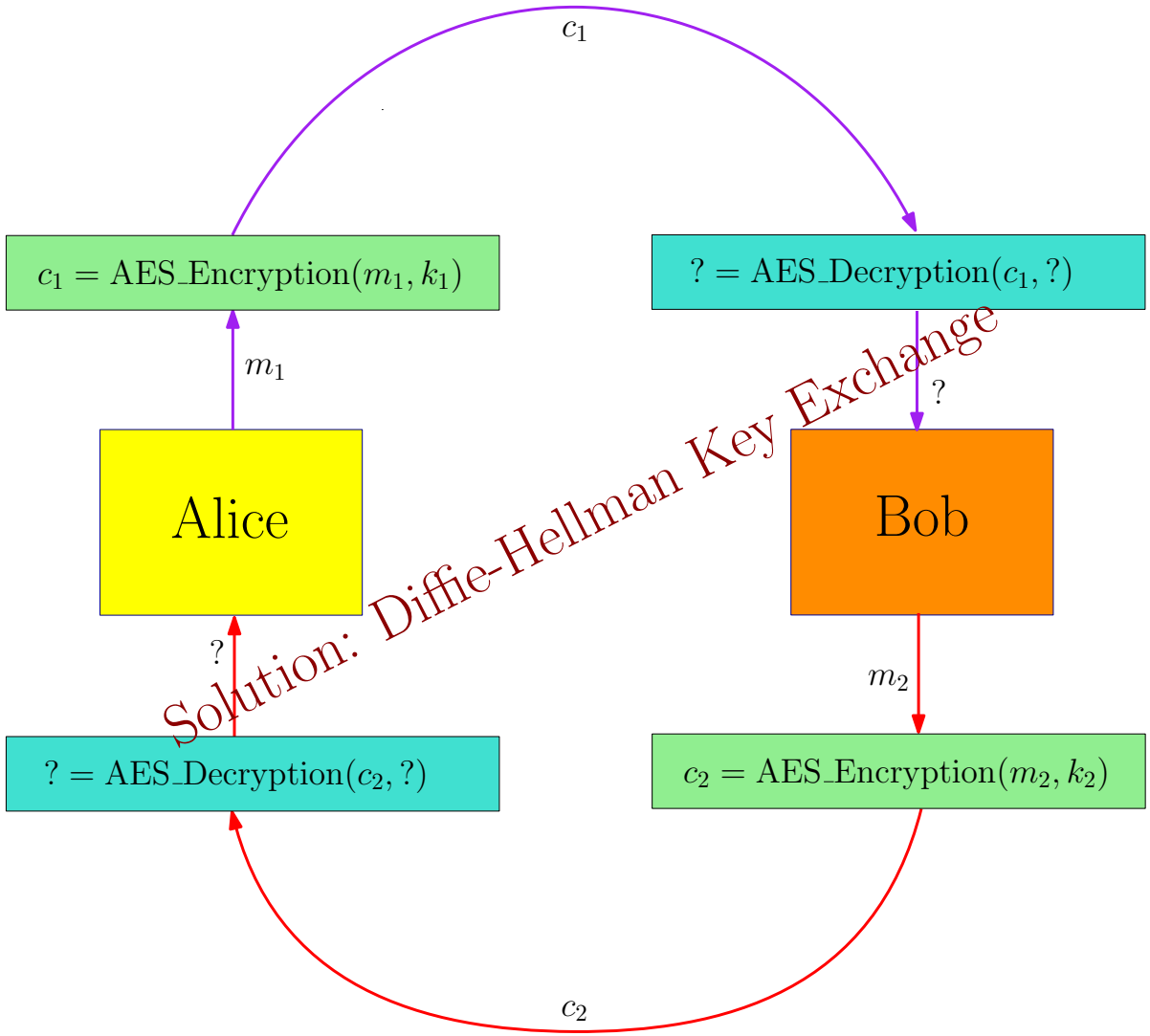


Figure: Secure Communication

Problem 1

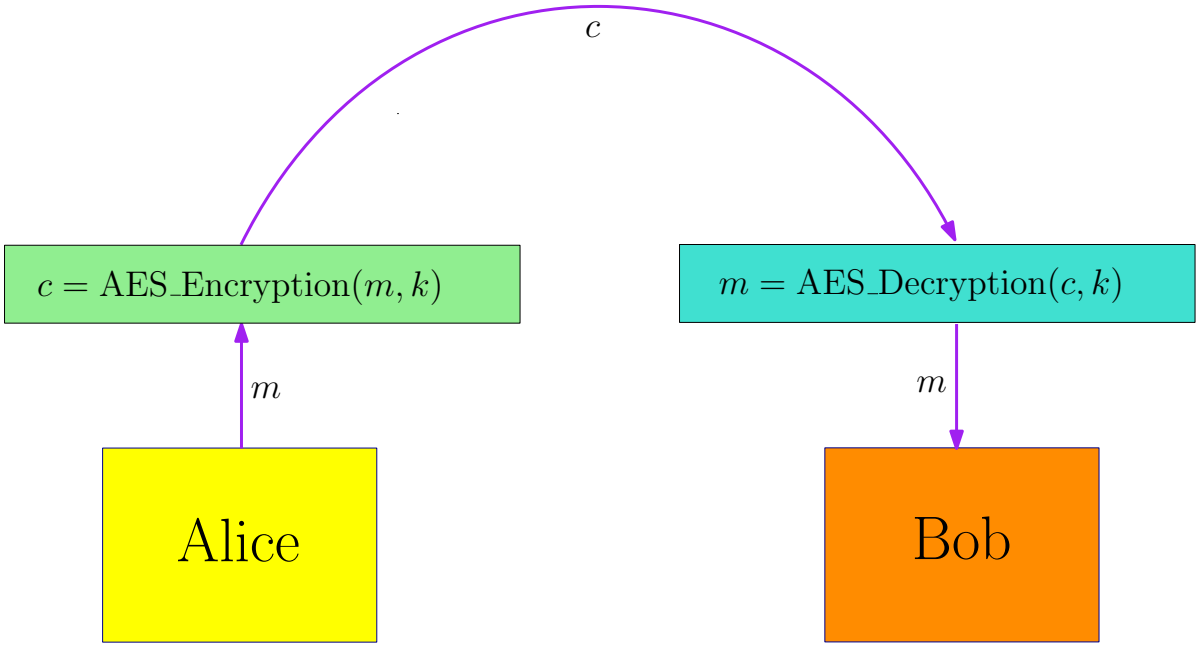
Introduction



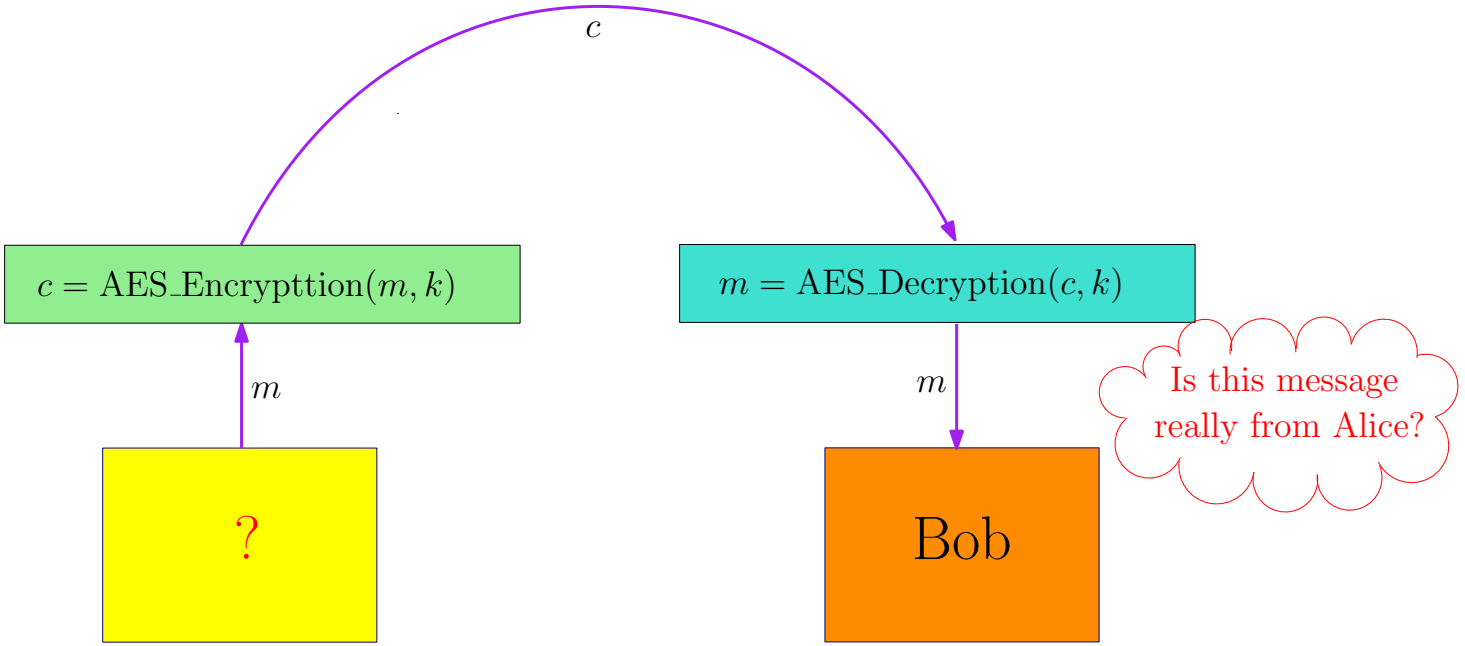


Problem 2

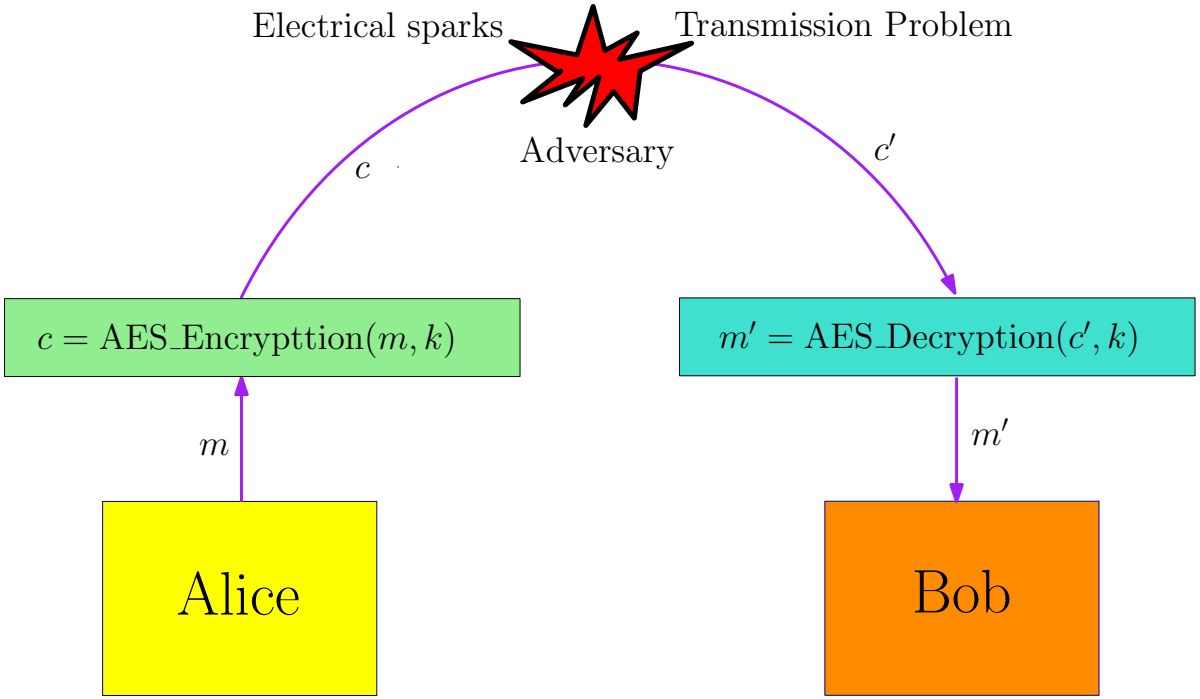
Introduction



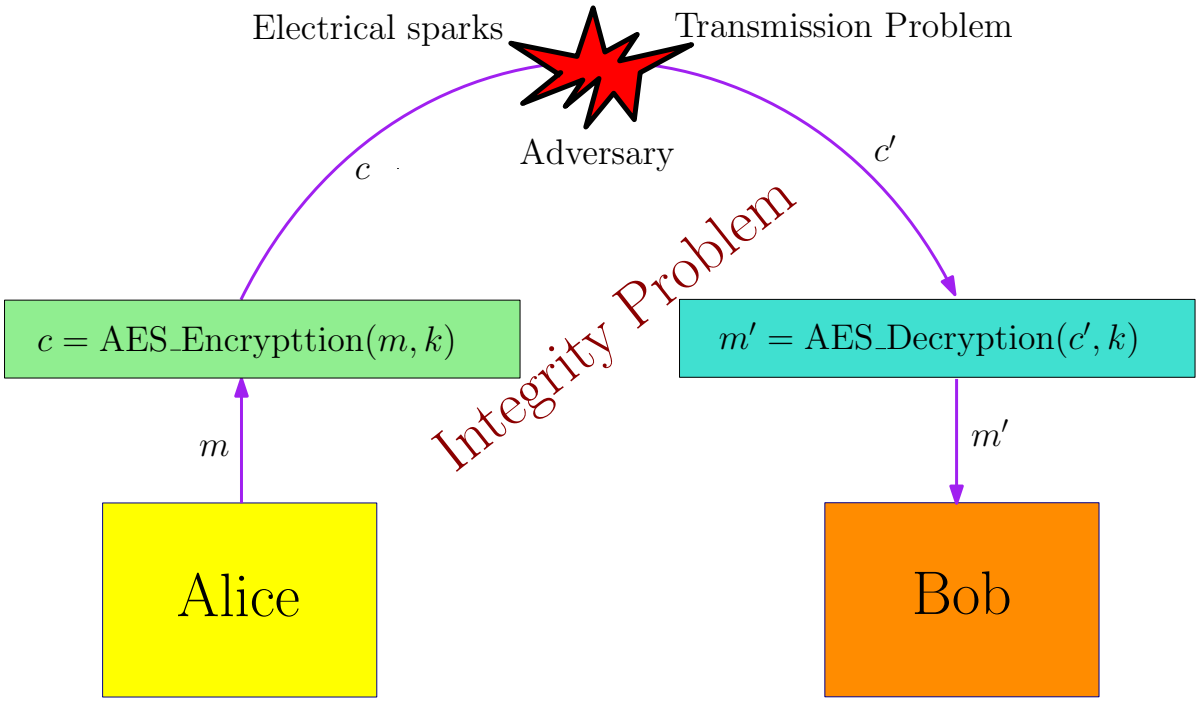
Introduction



- Case 1:

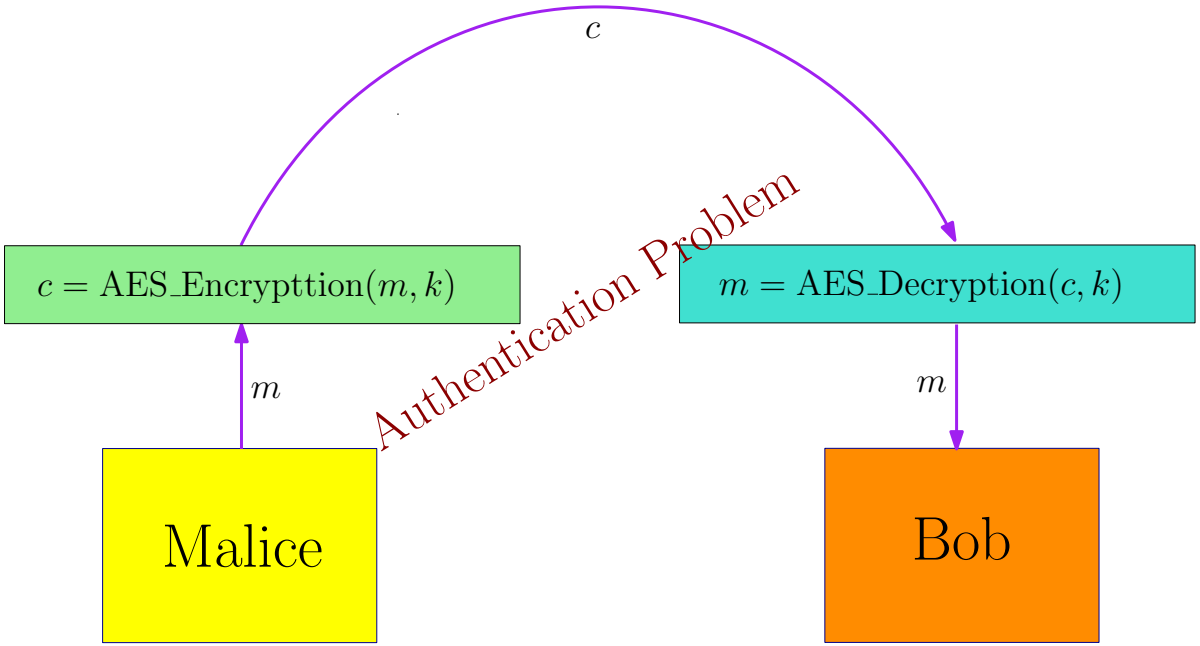


Introduction

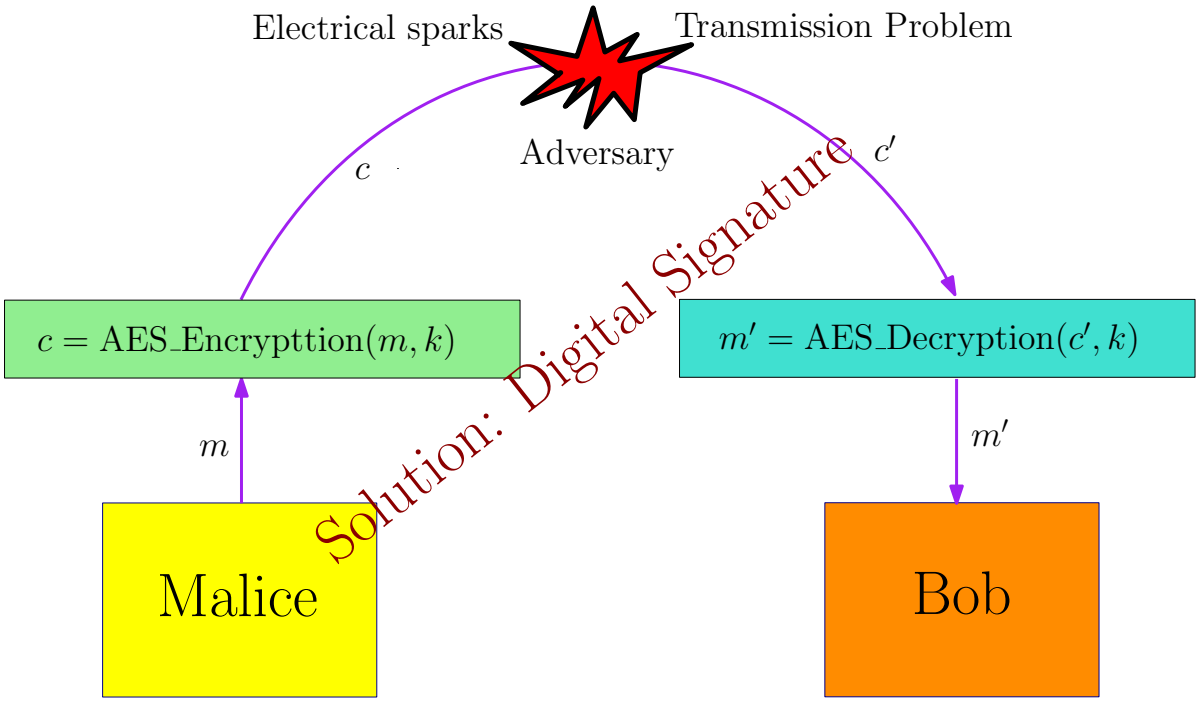


Introduction

- Case 2:



Introduction



Problem 3

Introduction

How to achieve privacy?

Introduction

How to achieve privacy?

Answer: Symmetric-Key Encryption Scheme

- Yesterday's Lecture by Dr. Rishiraj Bhattacharyya

Introduction

How to achieve privacy?

Answer: Symmetric-Key Encryption Scheme

- Yesterday's Lecture by Dr. Rishiraj Bhattacharyya

Is there any alternative?

Introduction

How to achieve privacy?

Answer: Symmetric-Key Encryption Scheme

- Yesterday's Lecture by Dr. Rishiraj Bhattacharyya

Is there any alternative?

Answer: Public-Key Encryption Scheme

Introduction

- In **Public-Key Cryptosystem**, each user has *two* types of *keys*
  - **Secret Key**: Only known to the user
  - **Public Key**: known to each and every user

Introduction

- In **Public-Key Cryptosystem**, each user has *two* types of *keys*
  - **Secret Key**: Only known to the user
  - **Public Key**: known to each and every user
- **Advantage**
  - Let the number of user be n
  - In Public-Key cryptosystem, total number of keys is $2n = O(n)$
  - In Symmetric-Key cryptosystem, total number of keys is $n(n-1)/2 = O(n^2)$

Introduction

- In **Public-Key Cryptosystem**, each user has *two* types of *keys*
  - **Secret Key**: Only known to the user
  - **Public Key**: known to each and every user
- **Advantage**
  - Let the number of user be n
  - In Public-Key cryptosystem, total number of keys is $2n = O(n)$
  - In Symmetric-Key cryptosystem, total number of keys is $n(n-1)/2 = O(n^2)$
- **Disadvantage**
  - Public-Key cryptosystem is significantly slower than Symmetric-Key cryptosystem

Introduction

1. Mathematical background

Introduction

1. Mathematical background
2. Diffie-Hellman Key Exchange

Introduction

1. Mathematical background
2. Diffie-Hellman Key Exchange
3. Digital Signature

Introduction

Introduction

Introduction

Outline for section 2

Notation

$\mathbb{N}$	Set of **Natural** Numbers	$\{1, 2, 3, \ldots\}$

Notation

$\mathbb{N}$	Set of **Natural** Numbers	$\{1, 2, 3, \ldots\}$
$\mathbb{Z}$	Set of **Integers**	$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

Notation

$\mathbb{N}$	Set of **Natural** Numbers	$\{1, 2, 3, \ldots\}$
$\mathbb{Z}$	Set of **Integers**	$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
$\mathbb{Z}^+$	Set of **Positive Integers**	$\{0, 1, 2, 3, \ldots\}$

Notation

$\mathbb{N}$	Set of **Natural** Numbers	$\{1, 2, 3, \ldots\}$
$\mathbb{Z}$	Set of **Integers**	$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
$\mathbb{Z}^+$	Set of **Positive Integers**	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{P}$	Set of (positive) **Prime** numbers	$\{2, 3, 5, \ldots\}$

Notation

$\mathbb{N}$	Set of **Natural** Numbers	$\{1, 2, 3, \ldots\}$
$\mathbb{Z}$	Set of **Integers**	$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
$\mathbb{Z}^+$	Set of **Positive Integers**	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{P}$	Set of (positive) **Prime** numbers	$\{2, 3, 5, \ldots\}$
$\mathbb{Q}$	Set of **Rational** numbers	$\left\{\frac{a}{b} \mid a \in \mathbb{Z} \text{ and } b \in \mathbb{N}\right\}$

Notation

$\mathbb{N}$	Set of **Natural** Numbers	$\{1, 2, 3, \ldots\}$
$\mathbb{Z}$	Set of **Integers**	$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
$\mathbb{Z}^+$	Set of **Positive Integers**	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{P}$	Set of (positive) **Prime** numbers	$\{2, 3, 5, \ldots\}$
$\mathbb{Q}$	Set of **Rational** numbers	$\left\{\frac{a}{b} \mid a \in \mathbb{Z} \text{ and } b \in \mathbb{N}\right\}$
$\mathbb{Q}^+$	Set of **Positive Rational** numbers	

Notation

$\mathbb{N}$	Set of **Natural** Numbers	$\{1, 2, 3, \ldots\}$
$\mathbb{Z}$	Set of **Integers**	$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
$\mathbb{Z}^+$	Set of **Positive Integers**	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{P}$	Set of (positive) **Prime** numbers	$\{2, 3, 5, \ldots\}$
$\mathbb{Q}$	Set of **Rational** numbers	$\left\{\frac{a}{b} \mid a \in \mathbb{Z} \text{ and } b \in \mathbb{N}\right\}$
$\mathbb{Q}^+$	Set of **Positive Rational** numbers	
$\mathbb{R}$	Set of **Real** numbers	

Notation

$\mathbb{N}$	Set of **Natural** Numbers	$\{1, 2, 3, \ldots\}$
$\mathbb{Z}$	Set of **Integers**	$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
$\mathbb{Z}^+$	Set of **Positive Integers**	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{P}$	Set of (positive) **Prime** numbers	$\{2, 3, 5, \ldots\}$
$\mathbb{Q}$	Set of **Rational** numbers	$\left\{\frac{a}{b} \mid a \in \mathbb{Z} \text{ and } b \in \mathbb{N}\right\}$
$\mathbb{Q}^+$	Set of **Positive Rational** numbers	
$\mathbb{R}$	Set of **Real** numbers	
$\mathbb{R}^+$	Set of **Positive Real** numbers	

Notation

$\mathbb{N}$	Set of **Natural** Numbers	$\{1, 2, 3, \ldots\}$
$\mathbb{Z}$	Set of **Integers**	$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
$\mathbb{Z}^+$	Set of **Positive Integers**	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{P}$	Set of (positive) **Prime** numbers	$\{2, 3, 5, \ldots\}$
$\mathbb{Q}$	Set of **Rational** numbers	$\left\{\frac{a}{b} \mid a \in \mathbb{Z} \text{ and } b \in \mathbb{N}\right\}$
$\mathbb{Q}^+$	Set of **Positive Rational** numbers	
$\mathbb{R}$	Set of **Real** numbers	
$\mathbb{R}^+$	Set of **Positive Real** numbers	

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

Euclidean Division Theorem

- Greek mathematician and philosopher Euclid (ca. 325–265 BC).

Division Theorem

For an integer a and an integer $b \neq 0$, there exist unique integers q and r such that

$$a = qb + r$$

with $0 \leqslant r <\mid b \mid$.

Euclidean Division Theorem

- Greek mathematician and philosopher Euclid (ca. 325–265 BC).

Division Theorem

For an integer a and an integer $b \neq 0$, there exist unique integers q and r such that

$$a = qb + r$$

with $0 \leqslant r <\mid b \mid$.

- q is called quotient and r is remainder
- Notation: $q = a$ quot b and $r = a$ rem b
- If $r = 0$, then $b \mid a$

Euclidean Division Theorem

- Greek mathematician and philosopher Euclid (ca. 325–265 BC).

Division Theorem

For an integer a and an integer $b \neq 0$, there exist unique integers q and r such that

$$a = qb + r$$

with $0 \leqslant r <\mid b \mid$.

- q is called quotient and r is remainder
- Notation: $q = a$ quot b and $r = a$ rem b
- If $r = 0$, then $b \mid a$

Examples

- $a = 10$ and $b = 4$, then $10 = 2 \times 4 + 2$
- $a = -10$ and $b = 4$, then $-10 = -3 \times 4 + 2$
- $a = 10$ and $b = 5$, then $5 \mid 10$

Greatest Common Divisor (gcd)

$\gcd(a,b) = d$

Let a and b be two non-zero integers. The largest positive integer d that divides both a and b is called the *greatest common divisor* or the gcd of a and b.

- $\gcd(a,b) = d$.
- $\gcd(a,b) = \gcd(b,a)$.
- For $a \neq 0$, $\gcd(a,0) = \mid a \mid$.
- $\gcd(0,0)$ is undefined.

Greatest Common Divisor (gcd)

$\gcd(a,b) = d$

Let a and b be two non-zero integers. The largest positive integer d that divides both a and b is called the *greatest common divisor* or the gcd of a and b.

- $\gcd(a,b) = d$.
- $\gcd(a,b) = \gcd(b,a)$.
- For $a \neq 0$, $\gcd(a,0) = \mid a \mid$.
- $\gcd(0,0)$ is undefined.

Bézout Relation

For $a, b \in \mathbb{Z}$, not both zero, $\exists\, u, v \in \mathbb{Z}$ such that $\gcd(a,b) = ua + vb$.

Greatest Common Divisor (gcd)

$\gcd(a,b) = d$

Let a and b be two non-zero integers. The largest positive integer d that divides both a and b is called the *greatest common divisor* or the gcd of a and b.

- $\gcd(a,b) = d$.
- $\gcd(a,b) = \gcd(b,a)$.
- For $a \neq 0$, $\gcd(a,0) = \mid a \mid$.
- $\gcd(0,0)$ is undefined.

Bézout Relation

For $a, b \in \mathbb{Z}$, not both zero, $\exists\, u, v \in \mathbb{Z}$ such that $\gcd(a,b) = ua + vb$.

Coprime

Two integers a, b are called *coprime* or *relatively prime* if $gcd(a,b) = 1$.

Greatest Common Divisor (gcd)

$\gcd(a,b) = d$

Let a and b be two non-zero integers. The largest positive integer d that divides both a and b is called the *greatest common divisor* or the gcd of a and b.

- $\gcd(a,b) = d$.
- $\gcd(a,b) = \gcd(b,a)$.
- For $a \neq 0$, $\gcd(a,0) = \mid a \mid$.
- $\gcd(0,0)$ is undefined.

Bézout Relation

For $a, b \in \mathbb{Z}$, not both zero, $\exists\, u, v \in \mathbb{Z}$ such that $\gcd(a,b) = ua + vb$.

Coprime

Two integers a, b are called *coprime* or *relatively prime* if $gcd(a,b) = 1$.

Examples

- $\gcd(15,20) = \gcd(20,15) = 5$
- $\gcd(6,35) = 1$

(Positive) Prime numbers ($\mathbb{P}$)

Prime

Let p be a positive integer and $p \neq 0, 1$. We say p is *prime* if $a \nmid p$ for all $1 < a < p$. Otherwise, p is a positive composite number.

(Positive) Prime numbers ($\mathbb{P}$)

Prime

Let p be a positive integer and $p \neq 0, 1$. We say p is *prime* if $a \nmid p$ for all $1 < a < p$. Otherwise, p is a positive composite number.

Alternative Definition

Let p be a positive integer and $p \neq 0, 1$. We say p is *prime* if p is coprime to all other integers which are not multiples of p.

(Positive) Prime numbers ($\mathbb{P}$)

Prime

Let p be a positive integer and $p \neq 0, 1$. We say p is *prime* if $a \nmid p$ for all $1 < a < p$. Otherwise, p is a positive composite number.

Alternative Definition

Let p be a positive integer and $p \neq 0, 1$. We say p is *prime* if p is coprime to all other integers which are not multiples of p.

Examples

- 7 is a prime number
- 6 is a composite as $6 = 2 \times 3$

Congruence

Let $m \in \mathbb{N}$. Two integers $a, b \in \mathbb{Z}$ are called congruent modulo m, denoted $a \equiv b \mod m$, if $m \mid (a - b)$ or, equivalently, if $a \text{ rem } m = b \text{ rem } m$. In this case, m is called the modulus of the congruence.

$$a \equiv b \mod m \Leftrightarrow m \mid (a - b) \Leftrightarrow a \text{ rem } m = b \text{ rem } m$$

Congruence

Let $m \in \mathbb{N}$. Two integers $a, b \in \mathbb{Z}$ are called congruent modulo m, denoted $a \equiv b \mod m$, if $m \mid (a - b)$ or, equivalently, if $a \text{ rem } m = b \text{ rem } m$. In this case, m is called the modulus of the congruence.

$$a \equiv b \mod m \Leftrightarrow m \mid (a - b) \Leftrightarrow a \text{ rem } m = b \text{ rem } m$$

Examples

- $a = 10$, $b = 4$, $m = 3$, then $10 \equiv 4 \mod 3$

Congruence

Let $m \in \mathbb{N}$. Two integers $a, b \in \mathbb{Z}$ are called congruent modulo m, denoted $a \equiv b \mod m$, if $m \mid (a - b)$ or, equivalently, if $a \text{ rem } m = b \text{ rem } m$. In this case, m is called the modulus of the congruence.

$$a \equiv b \mod m \Leftrightarrow m \mid (a - b) \Leftrightarrow a \text{ rem } m = b \text{ rem } m$$

Examples

- $a = 10$, $b = 4$, $m = 3$, then $10 \equiv 4 \mod 3$
- $3 \mid (10 - 4)$

Congruence

Let $m \in \mathbb{N}$. Two integers $a, b \in \mathbb{Z}$ are called congruent modulo m, denoted $a \equiv b \mod m$, if $m \mid (a - b)$ or, equivalently, if $a \text{ rem } m = b \text{ rem } m$. In this case, m is called the modulus of the congruence.

$$a \equiv b \mod m \Leftrightarrow m \mid (a - b) \Leftrightarrow a \text{ rem } m = b \text{ rem } m$$

Examples

- $a = 10$, $b = 4$, $m = 3$, then $10 \equiv 4 \mod 3$
- $3 \mid (10 - 4)$
- $10 \text{ rem } 3 = 4 \text{ rem } 3 = 1$

Congruence and Modular Arithmetic

Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$.

- $a \equiv a \mod m$.
- If $a \equiv b \mod m$, then $b \equiv a \mod m$.
- If $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$.
- If $a \equiv c \mod m$ and $b \equiv d \mod m$, then
  - $a + b \equiv c + d \mod m$
  - $a - b \equiv c - d \mod m$
  - $ab \equiv cd \mod m$

Representation

Let $m \in \mathbb{N}$, then $\mathbb{Z}_m$ is represented as

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

Arithmetic of $\mathbb{Z}_m$

Representation

Let $m \in \mathbb{N}$, then $\mathbb{Z}_m$ is represented as

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

Examples

For $m = 15$,

$$\mathbb{Z}_{15} = \{0, 1, 2, \ldots, 14\}$$

Arithmetic of $\mathbb{Z}_m$

Representation

Let $m \in \mathbb{N}$, then $\mathbb{Z}_m$ is represented as

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

Examples

For $m = 15$,

$$\mathbb{Z}_{15} = \{0, 1, 2, \ldots, 14\}$$

Addition on $\mathbb{Z}_m$

$$a + b = \begin{cases} a+b & \text{if } a+b < m \\ a+b-m & \text{if } a+b \geqslant m \end{cases}$$

Arithmetic of $\mathbb{Z}_m$

Representation

Let $m \in \mathbb{N}$, then $\mathbb{Z}_m$ is represented as

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

Examples

For $m = 15$,

$$\mathbb{Z}_{15} = \{0, 1, 2, \ldots, 14\}$$

Addition on $\mathbb{Z}_m$

$$a + b = \begin{cases} a+b & \text{if } a+b < m \\ a+b-m & \text{if } a+b \geqslant m \end{cases}$$

Examples

Let $m = 15$.

- If $a = 7$ and $b = 4$, then $a + b = 7 + 4 = 11 \mod 15$
- If $a = 11$ and $b = 13$, then $a + b = 11 + 13 - 15 = 9 \mod 15$

Subtraction on $\mathbb{Z}_m$

$$a - b = \begin{cases} a - b & \text{if } a \geqslant b \\ a - b + m & \text{if } a < b \end{cases}$$

Arithmetic of $\mathbb{Z}_m$

Subtraction on $\mathbb{Z}_m$

$$a - b = \begin{cases} a - b & \text{if } a \geqslant b \\ a - b + m & \text{if } a < b \end{cases}$$

Examples

Let $m = 15$.

- If $a = 7$ and $b = 4$, then $a - b = 7 - 4 = 3 \mod 15$
- If $a = 11$ and $b = 13$, then $a + b = 11 - 13 + 15 = 13 \mod 15$

Arithmetic of $\mathbb{Z}_m$

Subtraction on $\mathbb{Z}_m$

$$a - b = \begin{cases} a - b & \text{if } a \geqslant b \\ a - b + m & \text{if } a < b \end{cases}$$

Examples

Let $m = 15$.

- If $a = 7$ and $b = 4$, then $a - b = 7 - 4 = 3 \mod 15$
- If $a = 11$ and $b = 13$, then $a + b = 11 - 13 + 15 = 13 \mod 15$

Multiplication on $\mathbb{Z}_m$

$$a \cdot b = (ab) \text{ rem } m$$

Arithmetic of $\mathbb{Z}_m$

Subtraction on $\mathbb{Z}_m$

$$a - b = \begin{cases} a - b & \text{if } a \geqslant b \\ a - b + m & \text{if } a < b \end{cases}$$

Examples

Let $m = 15$.

- If $a = 7$ and $b = 4$, then $a - b = 7 - 4 = 3 \mod 15$
- If $a = 11$ and $b = 13$, then $a + b = 11 - 13 + 15 = 13 \mod 15$

Multiplication on $\mathbb{Z}_m$

$$a \cdot b = (ab) \text{ rem } m$$

Examples

Let $m = 15$.

- If $a = 7$ and $b = 4$, then $ab = (7 \times 4) \text{ rem } 15 = 28 \mod 15 = 13$

Identity

An element $e \in \mathbb{Z}_m$ is said to be

Additive identity : $a + e_1 \equiv e_1 + a \equiv a \mod m$, for all $a \in \mathbb{Z}_m$

Identity

An element $e \in \mathbb{Z}_m$ is said to be

$$\text{Additive identity} \quad : \quad a + e_1 \equiv e_1 + a \equiv a \mod m, \text{ for all } a \in \mathbb{Z}_m$$

$$\text{Multiplicative identity} \quad : \quad ae_2 \equiv e_2 a \equiv a \mod m, \text{ for all } a \in \mathbb{Z}_m$$

Arithmetic of $\mathbb{Z}_m$

Identity

An element $e \in \mathbb{Z}_m$ is said to be

$$\text{Additive identity} \quad : \quad a + e_1 \equiv e_1 + a \equiv a \mod m, \text{ for all } a \in \mathbb{Z}_m$$

$$\text{Multiplicative identity} \quad : \quad a e_2 \equiv e_2 a \equiv a \mod m, \text{ for all } a \in \mathbb{Z}_m$$

- $0 \in \mathbb{Z}_m$ is additive identity.
- $1 \in \mathbb{Z}_m$ is multiplicative identity.

Arithmetic of $\mathbb{Z}_m$

Identity

An element $e \in \mathbb{Z}_m$ is said to be

$$\text{Additive identity} \quad : \quad a + e_1 \equiv e_1 + a \equiv a \mod m, \text{ for all } a \in \mathbb{Z}_m$$
$$\text{Multiplicative identity} \quad : \quad ae_2 \equiv e_2 a \equiv a \mod m, \text{ for all } a \in \mathbb{Z}_m$$

- $0 \in \mathbb{Z}_m$ is additive identity.
- $1 \in \mathbb{Z}_m$ is multiplicative identity.

Invertible

An element $a \in \mathbb{Z}_m$ is said to be invertible modulo m if there exists an integer $u \in \mathbb{Z}_m$ such that $ua \equiv 1 \mod m$. u is called inverse of a denoted as a^{-1}.

Arithmetic of $\mathbb{Z}_m$

Identity

An element $e \in \mathbb{Z}_m$ is said to be

$$\text{Additive identity} \quad : \quad a + e_1 \equiv e_1 + a \equiv a \mod m, \text{ for all } a \in \mathbb{Z}_m$$
$$\text{Multiplicative identity} \quad : \quad a e_2 \equiv e_2 a \equiv a \mod m, \text{ for all } a \in \mathbb{Z}_m$$

- $0 \in \mathbb{Z}_m$ is additive identity.
- $1 \in \mathbb{Z}_m$ is multiplicative identity.

Invertible

An element $a \in \mathbb{Z}_m$ is said to be invertible modulo m if there exists an integer $u \in \mathbb{Z}_m$ such that $ua \equiv 1 \mod m$. u is called inverse of a denoted as a^{-1}.

Examples

Let $m = 15$.

- $a = 7$ is invertible as $7 \times 13 \equiv 1 \mod 15$
- $a = 6$ is not invertible.

Arithmetic of $\mathbb{Z}_m$

Identity

An element $e \in \mathbb{Z}_m$ is said to be

$$\text{Additive identity} \quad : \quad a + e_1 \equiv e_1 + a \equiv a \mod m, \text{ for all } a \in \mathbb{Z}_m$$
$$\text{Multiplicative identity} \quad : \quad ae_2 \equiv e_2 a \equiv a \mod m, \text{ for all } a \in \mathbb{Z}_m$$

- $0 \in \mathbb{Z}_m$ is additive identity.
- $1 \in \mathbb{Z}_m$ is multiplicative identity.

Invertible

An element $a \in \mathbb{Z}_m$ is said to be invertible modulo m if there exists an integer $u \in \mathbb{Z}_m$ such that $ua \equiv 1 \mod m$. u is called inverse of a denoted as a^{-1}.

Examples

Let $m = 15$.

- $a = 7$ is invertible as $7 \times 13 \equiv 1 \mod 15$
- $a = 6$ is not invertible.

Theorem

An element $a \in \mathbb{Z}_m$ is invertible if and only if $\gcd(a, m) = 1$.

Arithmetic of $\mathbb{Z}_m$

- $\phi(m)$ is known as **Euler's phi function** or **Euler's totient function**.
- $\phi(m) = |\{a \mid \gcd(a, m) = 1 \text{ and } 0 \leqslant a < m\}|$.

Arithmetic of $\mathbb{Z}_m$

- $\phi(m)$ is known as **Euler's phi function** or **Euler's totient function**.
- $\phi(m) = |\{a \mid \gcd(a,m) = 1 \text{ and } 0 \leqslant a < m\}|$.

Euler's product formula

Let $m = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of m with pair-wise distinct primes $p_1, \ldots, p_r$ and with each of $e_1, \ldots, e_r$ positive. Then,

$$\phi(m) = \left(p_1^{e_1} - p_1^{e_1-1}\right) \cdots \left(p_r^{e_r} - p_r^{e_r-1}\right) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right),$$

where the last product is over the set of all (distinct) prime divisors of m.

- $\phi(m)$ is known as **Euler's phi function** or **Euler's totient function**.
- $\phi(m) = |\{a \mid \gcd(a,m) = 1 \text{ and } 0 \leqslant a < m\}|$.

Euler's product formula

Let $m = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of m with pair-wise distinct primes $p_1, \ldots, p_r$ and with each of $e_1, \ldots, e_r$ positive. Then,

$$\phi(m) = \left(p_1^{e_1} - p_1^{e_1-1}\right) \cdots \left(p_r^{e_r} - p_r^{e_r-1}\right) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right),$$

where the last product is over the set of all (distinct) prime divisors of m.

Examples

For $m = 15$,

- $15 = 3^1 \times 5^1$
- $\phi(15) = \left(3^1 - 3^0\right)\left(5^1 - 5^0\right) = 2 \times 4 = 8.$

Structure of $\mathbb{Z}_m^*$

There are $\phi(m)$ elements in $\mathbb{Z}_m$ which are coprime to m

Examples

- $\phi(15) = 8$
- Coprimes are $\{1, 2, 4, 7, 8, 11, 13, 14\}$.

Structure of $\mathbb{Z}_m^*$

There are $\phi(m)$ elements in $\mathbb{Z}_m$ which are coprime to m

Examples

- $\phi(15) = 8$
- Coprimes are $\{1, 2, 4, 7, 8, 11, 13, 14\}$.

$\mathbb{Z}_m^*$

$$\mathbb{Z}_m^* = \{a \mid 0 \leqslant a < m \text{ and } \gcd(a, m) = 1\}.$$

Structure of $\mathbb{Z}_m^*$

There are $\phi(m)$ elements in $\mathbb{Z}_m$ which are coprime to m

Examples

- $\phi(15) = 8$
- Coprimes are $\{1, 2, 4, 7, 8, 11, 13, 14\}$.

$\mathbb{Z}_m^*$

$$\mathbb{Z}_m^* = \{a \mid 0 \leqslant a < m \text{ and } \gcd(a, m) = 1\}.$$

Examples

$$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

Structure of $\mathbb{Z}_m^*$

Euler's theorem

Let $m \in \mathbb{N}$ and $\gcd(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \mod m$.

Structure of $\mathbb{Z}_m^*$

Euler's theorem

Let $m \in \mathbb{N}$ and $\gcd(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \mod m$.

Examples

- $a \in \mathbb{Z}_m^*$, $a^{\phi(m)} \equiv 1 \mod m$
- Let $m = 15$ and $a = 4$, them $4^8 = 65536 \equiv 1 \mod 15$ as $65536 = 4369 \times 15 + 1$.
- $a \in \mathbb{Z}_m^*$, $aa^{\phi(m)-1} \equiv 1 \mod m$, then $a^{-1} \equiv a^{\phi(m)-1} \mod m$

Structure of $\mathbb{Z}_m^*$

Euler's theorem

Let $m \in \mathbb{N}$ and $\gcd(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \mod m$.

Examples

- $a \in \mathbb{Z}_m^*$, $a^{\phi(m)} \equiv 1 \mod m$
- Let $m = 15$ and $a = 4$, them $4^8 = 65536 \equiv 1 \mod 15$ as $65536 = 4369 \times 15 + 1$.
- $a \in \mathbb{Z}_m^*$, $aa^{\phi(m)-1} \equiv 1 \mod m$, then $a^{-1} \equiv a^{\phi(m)-1} \mod m$

Fermat's little theorem

Let $p \in \mathbb{P}$, and a an integer not divisible by p. Then, $a^{p-1} \equiv 1 \mod p$. For any integer b, we have $b^p \equiv b \mod p$.

Binary Operation

Binary Operation

A *binary operation* $\circ$ on a set G is a map from $G \times G$ to G, that is

$$\circ : G \times G \mapsto G.$$

Binary Operation

Binary Operation

A *binary operation* $\circ$ on a set G is a map from $G \times G$ to G, that is

$$\circ : G \times G \mapsto G.$$

Examples

Addition, subtraction and multiplication on $\mathbb{Z}_m$.

Group

Group

Let G be a set with binary operation $\circ$. $(G, \circ)$ is called a group if it satisfies the following conditions:

- **Associative**: $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$.

Group

Group

Let G be a set with binary operation $\circ$. $(G, \circ)$ is called a group if it satisfies the following conditions:

- **Associative**: $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$.
- **Identity**: $\exists$ an unique element $e \in G$ such that $a \circ e = e \circ a = a$, $\forall a \in G$. The element e is called Identity of G.

Group

Group

Let G be a set with binary operation $\circ$. $(G, \circ)$ is called a group if it satisfies the following conditions:

- **Associative**: $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$.
- **Identity**: $\exists$ an unique element $e \in G$ such that $a \circ e = e \circ a = a$, $\forall a \in G$. The element e is called Identity of G.
- **Inverse**: $a \in G$, $\exists$ an unique element $b \in G$ such that $a \circ b = b \circ a = e$. The element b is called Inverse of a.

Group

Group

Let G be a set with binary operation $\circ$. $(G, \circ)$ is called a group if it satisfies the following conditions:

- **Associative**: $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$.
- **Identity**: $\exists$ an unique element $e \in G$ such that $a \circ e = e \circ a = a$, $\forall a \in G$. The element e is called Identity of G.
- **Inverse**: $a \in G$, $\exists$ an unique element $b \in G$ such that $a \circ b = b \circ a = e$. The element b is called Inverse of a.

Commutative or Abelian Group

A group $(G, \circ)$ is called commutative or abelian if for all $a, b \in G$

$$a \circ b = b \circ a.$$

Group

Group

Let G be a set with binary operation $\circ$. $(G, \circ)$ is called a group if it satisfies the following conditions:

- **Associative**: $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$.
- **Identity**: $\exists$ an unique element $e \in G$ such that $a \circ e = e \circ a = a$, $\forall a \in G$. The element e is called Identity of G.
- **Inverse**: $a \in G$, $\exists$ an unique element $b \in G$ such that $a \circ b = b \circ a = e$. The element b is called Inverse of a.

Commutative or Abelian Group

A group $(G, \circ)$ is called commutative or abelian if for all $a, b \in G$

$$a \circ b = b \circ a.$$

Examples

- $(\mathbb{Z}_m, +)$ and $(\mathbb{Z}_m^*, \cdot)$

Group

Order

- The order of the group G, denoted by $O(G)$, is simply the number of elements in G.
- The order of an element in a group G (notation $O(a)$) is the least positive integer n such that $a^n = 1$.

Group

Order

- The order of the group G, denoted by $O(G)$, is simply the number of elements in G.
- The order of an element in a group G (notation $O(a)$) is the least positive integer n such that $a^n = 1$.

Subgroup

Let $(G, \circ)$ be group and H be a non-empty subset of G. If $(H, \circ)$ is also a group, then H is subgroup of G.

Group

Order

- The order of the group G, denoted by $O(G)$, is simply the number of elements in G.
- The order of an element in a group G (notation $O(a)$) is the least positive integer n such that $a^n = 1$.

Subgroup

Let $(G, \circ)$ be group and H be a non-empty subset of G. If $(H, \circ)$ is also a group, then H is subgroup of G.

Lagrange's Theorem

Let $(G, \circ)$ be a finite group and H be a subgroup of G. Then $O(H) \mid O(G)$.

Group

Order

- The order of the group G, denoted by $O(G)$, is simply the number of elements in G.
- The order of an element in a group G (notation $O(a)$) is the least positive integer n such that $a^n = 1$.

Subgroup

Let $(G, \circ)$ be group and H be a non-empty subset of G. If $(H, \circ)$ is also a group, then H is subgroup of G.

Lagrange's Theorem

Let $(G, \circ)$ be a finite group and H be a subgroup of G. Then $O(H) \mid O(G)$.

Examples

- $(\mathbb{Z}_{15}^*, \cdot)$ is group
- $(1, \cdot)$ is subgroup of $\mathbb{Z}_{15}^*$
- $H = \{1, 2, 4, 8\}$ is also a subgroup of $\mathbb{Z}_{15}^*$

Group

Cyclic Group

Let $(G, \circ)$ be a group. G is called cyclic if there exists $a \in G$ such that

$$G = \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle.$$

Group

Cyclic Group

Let $(G, \circ)$ be a group. G is called cyclic if there exists $a \in G$ such that

$$G = \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle.$$

- Let $(G, \circ)$ be a group and $a \in G$ with order n. Then $\langle a \rangle$ is a cyclic subgroup of G.

Examples

- $G = \mathbb{Z}_{15}^*$ and $H = \{1, 2, 4, 8\}$.
- $O(G) = \phi(15) = 8$
- $O(2) = 4$.
- $H = \langle 2 \rangle = \{2^0, 2^1, 2^2, 2^3\} = \{1, 2, 4, 8\}$.

Group

Theorem

Each cyclic group is abelian.

Theorem

If $(G, \cdot)$ is a finite group and order of it is a prime, then G is cyclic.

Outline for section 3

Diffie-Hellman Key Exchange

- Introduced by Whitfield **Diffie** and Martin **Hellman** in 1976.

Diffie-Hellman Key Exchange

- Introduced by Whitfield **Diffie** and Martin **Hellman** in 1976.

Domain Parameter

- Let G be an abelian group of order n
- Let $g \in G$ such that $\langle g \rangle$ is the largest prime subgroup of G.
- Let $O(g) = m$

Diffie-Hellman Key Exchange

- Introduced by Whitfield **Diffie** and Martin **Hellman** in 1976.

Domain Parameter

- Let G be an abelian group of order n
- Let $g \in G$ such that $\langle g \rangle$ is the largest prime subgroup of G.
- Let $O(g) = m$

Diffie-Hellman Key Exchange

Alice	Bob

Diffie-Hellman Key Exchange

- Introduced by Whitfield **Diffie** and Martin **Hellman** in 1976.

Domain Parameter

- Let G be an abelian group of order n
- Let $g \in G$ such that $\langle g \rangle$ is the largest prime subgroup of G.
- Let $O(g) = m$

Diffie-Hellman Key Exchange

Alice	Bob
1. $a \in_R \{2, 3, \ldots, m-1\}$	1. $b \in_R \{2, 3, \ldots, m-1\}$

Diffie-Hellman Key Exchange

- Introduced by Whitfield **Diffie** and Martin **Hellman** in 1976.

Domain Parameter

- Let G be an abelian group of order n
- Let $g \in G$ such that $\langle g \rangle$ is the largest prime subgroup of G.
- Let $O(g) = m$

Diffie-Hellman Key Exchange

Alice	Bob
1. $a \in_R \{2, 3, \ldots, m-1\}$	1. $b \in_R \{2, 3, \ldots, m-1\}$
2. Computes $A = g^a$	2. Computes $B = g^b$

Diffie-Hellman Key Exchange

- Introduced by Whitfield **Diffie** and Martin **Hellman** in 1976.

Domain Parameter

- Let G be an abelian group of order n
- Let $g \in G$ such that $\langle g \rangle$ is the largest prime subgroup of G.
- Let $O(g) = m$

Diffie-Hellman Key Exchange

Alice		Bob
1. $a \in_R \{2, 3, \ldots, m-1\}$		1. $b \in_R \{2, 3, \ldots, m-1\}$
2. Computes $A = g^a$		2. Computes $B = g^b$
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	

Diffie-Hellman Key Exchange

- Introduced by Whitfield **Diffie** and Martin **Hellman** in 1976.

Domain Parameter

- Let G be an abelian group of order n
- Let $g \in G$ such that $\langle g \rangle$ is the largest prime subgroup of G.
- Let $O(g) = m$

Diffie-Hellman Key Exchange

Alice		Bob
1. $a \in_R \{2, 3, \ldots, m-1\}$		1. $b \in_R \{2, 3, \ldots, m-1\}$
2. Computes $A = g^a$		2. Computes $B = g^b$
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	
3. Computes $K = B^a = g^{ab}$		3. Computes $K = A^b = g^{ab}$

Diffie-Hellman Key Exchange

Domain Parameter

- Let $G = \mathbb{Z}_p^*$ where $p = 35394171431 \in \mathbb{P}$
- Let $g = 180$ and $O(g) = 122048867 \in \mathbb{P}$

Diffie-Hellman Key Exchange

Domain Parameter

- Let $G = \mathbb{Z}_p^*$ where $p = 35394171431 \in \mathbb{P}$
- Let $g = 180$ and $O(g) = 122048867 \in \mathbb{P}$

Diffie-Hellman Key Exchange

Alice	Bob

Diffie-Hellman Key Exchange

Domain Parameter

- Let $G = \mathbb{Z}_p^*$ where $p = 35394171431 \in \mathbb{P}$
- Let $g = 180$ and $O(g) = 122048867 \in \mathbb{P}$

Diffie-Hellman Key Exchange

Alice	Bob
1. $a = 96642237$	1. $b = 54986757$

Diffie-Hellman Key Exchange

Domain Parameter

- Let $G = \mathbb{Z}_p^*$ where $p = 35394171431 \in \mathbb{P}$
- Let $g = 180$ and $O(g) = 122048867 \in \mathbb{P}$

Diffie-Hellman Key Exchange

Alice	Bob
1. $a = 96642237$	1. $b = 54986757$
2. $A = g^a = 14631136677$	2. $B = g^b = 23989781989$

Diffie-Hellman Key Exchange

Domain Parameter

- Let $G = \mathbb{Z}_p^*$ where $p = 35394171431 \in \mathbb{P}$
- Let $g = 180$ and $O(g) = 122048867 \in \mathbb{P}$

Diffie-Hellman Key Exchange

Alice		Bob
1. $a = 96642237$		1. $b = 54986757$
2. $A = g^a = 14631136677$		2. $B = g^b = 23989781989$
	$\xrightarrow{14631136677}$	
	$\xleftarrow{23989781989}$	

Diffie-Hellman Key Exchange

Domain Parameter

- Let $G = \mathbb{Z}_p^*$ where $p = 35394171431 \in \mathbb{P}$
- Let $g = 180$ and $O(g) = 122048867 \in \mathbb{P}$

Diffie-Hellman Key Exchange

Alice		Bob
1. $a = 96642237$		1. $b = 54986757$
2. $A = g^a = 14631136677$		2. $B = g^b = 23989781989$
	$\xrightarrow{14631136677}$	
	$\xleftarrow{23989781989}$	
3. $K = B^a = 30864161233$		3. $K = A^b = 3086416123$

Intractable problems

From a computational complexity stance, intractable problems are problems for which there exist no efficient algorithms to solve them. Therefore, it is not feasible for computation with anything more than the smallest input.

Intractable problems

From a computational complexity stance, intractable problems are problems for which there exist no efficient algorithms to solve them. Therefore, it is not feasible for computation with anything more than the smallest input.

Discrete Logarithm Problem (DLP)

Let G be a multiplicative group and let $g \in G$. Given g and g^a for some (unknown) integer a, compute a.

Intractable problems

From a computational complexity stance, intractable problems are problems for which there exist no efficient algorithms to solve them. Therefore, it is not feasible for computation with anything more than the smallest input.

Discrete Logarithm Problem (DLP)

Let G be a multiplicative group and let $g \in G$. Given g and g^a for some (unknown) integer a, compute a.

Diffie-Hellman Problem (DHP)

Let G be a multiplicative group and let $g \in G$. Given g, g^a and g^b for some (unknown) integers a and b, compute g^{ab}.

Diffie-Hellman Key Exchange

Intractable problems

From a computational complexity stance, intractable problems are problems for which there exist no efficient algorithms to solve them. Therefore, it is not feasible for computation with anything more than the smallest input.

Discrete Logarithm Problem (DLP)

Let G be a multiplicative group and let $g \in G$. Given g and g^a for some (unknown) integer a, compute a.

Diffie-Hellman Problem (DHP)

Let G be a multiplicative group and let $g \in G$. Given g, g^a and g^b for some (unknown) integers a and b, compute g^{ab}.

Decisional Diffie-Hellman Problem (DDHP)

Let G be a multiplicative group and let $g \in G$ with $O(g) = m$. Given g, g^a, g^b and g^c for some (unknown) integers a, b and c, decides whether $c \stackrel{?}{\equiv} ab \mod m$.

Outline for section 4

Digital Signature

- Digital Signature: {Key Generation, Signing, Verification}.
- Key Generation: Probabilistic Polynomial-time (PPT) algorithm.
- Signing: PPT algorithm.
- Verification: Deterministic Polynomial-time algorithm.

Digital Signature

- Digital Signature: {Key Generation, Signing, Verification}.
- Key Generation: Probabilistic Polynomial-time (PPT) algorithm.
- Signing: PPT algorithm.
- Verification: Deterministic Polynomial-time algorithm.

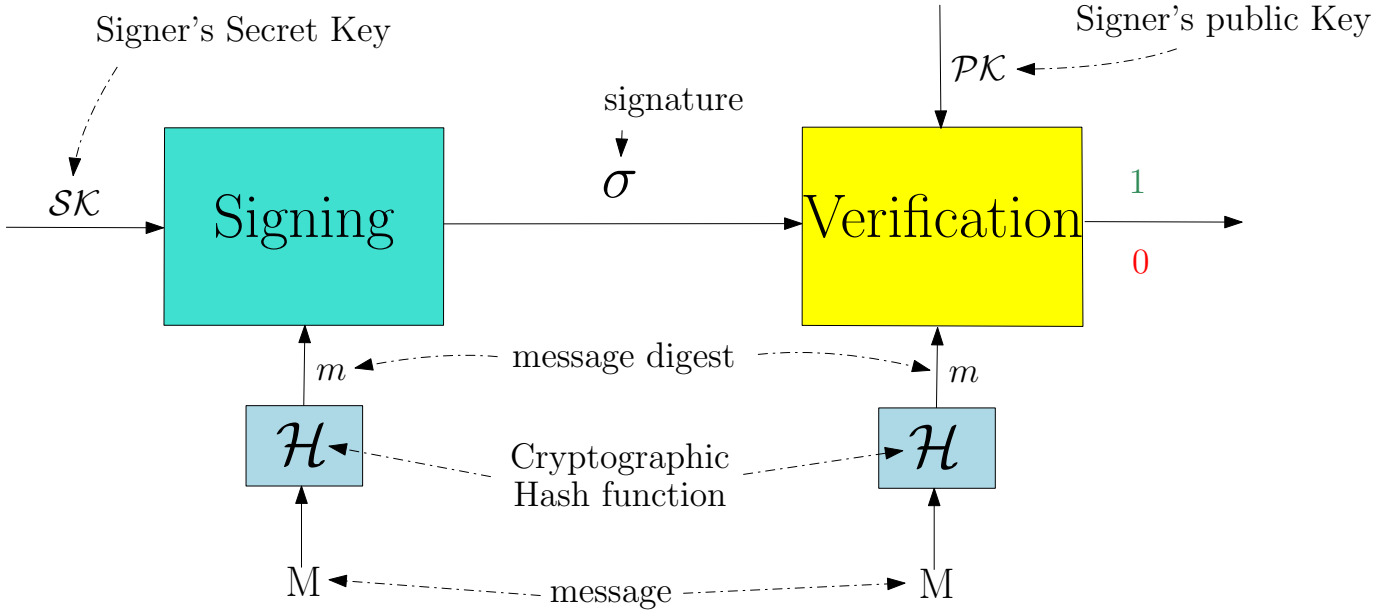


Figure: Digital Signature

RSA Digital Signature

- Introduced by Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman in 1977

Key Generation

1. Let the security parameter be l
2. Choose two primes p and q of bit-length almost l
3. Compute $n = pq$ and $\phi(n) = (p-1)(q-1)$
4. Choose e such that $\gcd(e, \phi(n)) = 1$
5. Compute $d \equiv e^{-1} \mod \phi(n)$
6. $\mathcal{SK} = d$ and $\mathcal{PK} = (n, e)$

RSA Digital Signature

Signing($M, \mathcal{SK}$)

1. Compute $m = \mathcal{H}(M) \in \mathbb{Z}_n^*$.
2. Compute $\sigma \equiv m^d \mod n$.

RSA Digital Signature

Signing($M, \mathcal{SK}$)

1. Compute $m = \mathcal{H}(M) \in \mathbb{Z}_n^*$.
2. Compute $\sigma \equiv m^d \mod n$.

Verification($M, \sigma, \mathcal{PK}$)

1. Compute $m = \mathcal{H}(M) \in \mathbb{Z}_n^*$.
2. Compute $m' \equiv \sigma^e \mod n$.
3. Check $m \stackrel{?}{=} m'$.
4. If $m = m'$, Return 1, else 0.

RSA Digital Signature

Signing($M, \mathcal{SK}$)

1. Compute $m = \mathcal{H}(M) \in \mathbb{Z}_n^*$.
2. Compute $\sigma \equiv m^d \mod n$.

Verification($M, \sigma, \mathcal{PK}$)

1. Compute $m = \mathcal{H}(M) \in \mathbb{Z}_n^*$.
2. Compute $m' \equiv \sigma^e \mod n$.
3. Check $m \stackrel{?}{=} m'$.
4. If $m = m'$, Return 1, else 0.

Correctness

$$m' \equiv \sigma^e \equiv (m^d)^e \equiv m^{ed} \equiv m \mod n,$$

as

$$ed \equiv 1 \mod \phi(n).$$

Key Generation

1. security parameter $l = 18$
2. $p = 241537$ and $q = 382069$
3. $n = pq = 92283800053$
4. $\phi(n) = (241537 - 1)(382069 - 1) = 92283176448$
5. $e = 5$
6. $d \equiv e^{-1} \equiv 55369905869 \mod \phi(n)$
7. $\mathcal{SK} = 55369905869$ and $\mathcal{PK} = (92283800053, 5)$

Signing($M, \mathcal{SK}$)

1. $m = \mathcal{H}(M) = 1234567890 \in \mathbb{Z}_n^*$
2. $\sigma \equiv m^d \equiv 85505674365 \mod n$

RSA Digital Signature

Signing($M, \mathcal{SK}$)

1. $m = \mathcal{H}(M) = 1234567890 \in \mathbb{Z}_n^*$
2. $\sigma \equiv m^d \equiv 85505674365 \mod n$

Verification($M, \sigma, \mathcal{PK}$)

1. $m = \mathcal{H}(M) = 1234567890 \in \mathbb{Z}_n^*$
2. $m' \equiv \sigma^e \equiv 1234567890 \mod n$
3. $m \stackrel{?}{=} m'$
4. As $m = m'$, Return 1

Security of RSA

Intractable problems

- Integer Factorization.
- RSA Key Inversion problem

ElGamal Digital Signature

- ElGamal signature scheme was introduced by Tahir Elgamal in 1985.

Domain parameter

- Let G be a cyclic multiplicative group.
- $O(G) = n$
- $\exists g \in G$ such that $G = \langle g \rangle$ and $O(g) = n$

- ElGamal signature scheme was introduced by Tahir Elgamal in 1985.

Domain parameter

- Let G be a cyclic multiplicative group.
- $O(G) = n$
- $\exists g \in G$ such that $G = \langle g \rangle$ and $O(g) = n$

Key Generation

- Choose $d \in_R \{2, \ldots, n-1\}$
- Compute $Q \equiv g^d$
- $\mathcal{SK} = d$ and $\mathcal{PK} = Q$

Signing($M, \mathcal{SK}$)

1. Choose $k \in_R \{2, \ldots, n-1\}$
2. Compute $m = \mathcal{H}(M) \in G$
3. Compute $s = g^k$
4. Compute $t \equiv k^{-1}(m - ds)$
5. Signature $\sigma = (s, t)$

Signing($M, \mathcal{SK}$)

1. Choose $k \in_R \{2, \ldots, n-1\}$
2. Compute $m = \mathcal{H}(M) \in G$
3. Compute $s = g^k$
4. Compute $t \equiv k^{-1}(m - ds)$
5. Signature $\sigma = (s, t)$

Verification($M, \sigma, \mathcal{PK}$)

1. Compute $m = \mathcal{H}(M) \in G$
2. Compute $a_1 = g^m$
3. Compute $a_2 = Q^s s^t$
4. Check $a_1 \stackrel{?}{=} a_2$.
5. If yes Return 1, else Return 0

Signing($M, \mathcal{SK}$)

1. Choose $k \in_R \{2, \ldots, n-1\}$
2. Compute $m = \mathcal{H}(M) \in G$
3. Compute $s = g^k$
4. Compute $t \equiv k^{-1}(m - ds)$
5. Signature $\sigma = (s, t)$

Verification($M, \sigma, \mathcal{PK}$)

1. Compute $m = \mathcal{H}(M) \in G$
2. Compute $a_1 = g^m$
3. Compute $a_2 = Q^s s^t$
4. Check $a_1 \stackrel{?}{=} a_2$.
5. If yes Return 1, else Return 0

Correctness

$$a_1 \equiv g^m \equiv g^{tk+ds} = (g^k)^t (g^d)^s \equiv s^t Q^s = a_2$$

Domain parameter

- $G = \mathbb{Z}_p^*$ where $p = 92283800099$
- $n = O(G) = 92283800098$
- $g = 19$ and $O(g) = 92283800098$

Domain parameter

- $G = \mathbb{Z}_p^*$ where $p = 92283800099$
- $n = O(G) = 92283800098$
- $g = 19$ and $O(g) = 92283800098$

Key Generation

- $d = 23499347910$
- $Q \equiv g^d \equiv 66075503407 \mod p$
- $\mathcal{SK} = 23499347910$ and $\mathcal{PK} = 66075503407$

Signing($M, \mathcal{SK}$)

1. $k = 9213753243$
2. $m = \mathcal{H}(M) = 1234567890$
3. $s \equiv g^k \equiv 85536409136 \mod p$
4. $t \equiv k^{-1}(m - ds) \equiv 22134180366 \mod \phi(p)$
5. $\sigma = (85536409136, 22134180366)$

Signing($M, \mathcal{SK}$)

1. $k = 9213753243$
2. $m = \mathcal{H}(M) = 1234567890$
3. $s \equiv g^k \equiv 85536409136 \mod p$
4. $t \equiv k^{-1}(m - ds) \equiv 22134180366 \mod \phi(p)$
5. $\sigma = (85536409136, 22134180366)$

Verification($M, \sigma, \mathcal{PK}$)

1. $m = \mathcal{H}(M) = 1234567890$
2. $a_1 = g^m \equiv 44505409554 \mod p$
3. $a_2 = Q^s s^t \equiv 44505409554 \mod p$
4. As $a_1 = a_2$, Return 1.

- National Institute of Standards and Technology (NIST) proposed DSA in 1991

Domain parameter(p, q, g)

- Let $G = \mathbb{Z}_p^*$ for some prime p
- Let $g \in G$ such that $\langle g \rangle$ is the largest prime subgroup of G.
- Let $O(g) = q$

DSA Digital Signature

- National Institute of Standards and Technology (NIST) proposed DSA in 1991

Domain parameter(p, q, g)

- Let $G = \mathbb{Z}_p^*$ for some prime p
- Let $g \in G$ such that $\langle g \rangle$ is the largest prime subgroup of G.
- Let $O(g) = q$

Key Generation

- Choose $d \in_R \{2, \ldots, q-1\}$.
- Compute $Q \equiv g^d \mod p$
- $\mathcal{SK} = d$ and $\mathcal{PK} = Q$

Signing($M, \mathcal{SK}$)

1. Choose $k \in_R \{2, 3, \ldots, q-1\}$
2. Compute $m = \mathcal{H}(M) \in \mathbb{Z}_p$
3. Compute $s = \left(g^k \mod p\right) \mod q$
4. Compute $t = k^{-1}(m + ds) \mod q$
5. Signature $\sigma = (s, t)$

Signing$(M, \mathcal{SK})$

1. Choose $k \in_R \{2, 3, \ldots, q-1\}$
2. Compute $m = \mathcal{H}(M) \in \mathbb{Z}_p$
3. Compute $s = \left(g^k \mod p\right) \mod q$
4. Compute $t = k^{-1}(m + ds) \mod q$
5. Signature $\sigma = (s, t)$

Verification$(M, \sigma, \mathcal{PK})$

1. Compute $m = \mathcal{H}(M) \in \mathbb{Z}_p$
2. Compute $w \equiv t^{-1} \mod q$
3. Compute $w_1 \equiv mw \mod q$
4. Compute $w_2 \equiv sw \mod q$
5. Compute $s' = (g^{w_1} Q^{w_2} \mod p) \mod q$
6. Check $s' \stackrel{?}{=} s$; If yes Return 1, else Return 0.

Correctness

$$s' = g^{w_1} Q^{w_2}$$

Correctness

$$\begin{aligned} s' &= g^{w_1} Q^{w_2} \\ &= g^{w_1} g^{d w_2} \qquad \text{as } Q = g^d \end{aligned}$$

Correctness

$$
\begin{aligned}
s' &= g^{w_1} Q^{w_2} \\
&= g^{w_1} g^{dw_2} && \text{as } Q = g^d \\
&= g^{wm} g^{dsw} && \text{as } w_1 = mw \text{ and } w_2 = sw
\end{aligned}
$$

Correctness

$$
\begin{aligned}
s' &= g^{w_1} Q^{w_2} \\
&= g^{w_1} g^{dw_2} && \text{as } Q = g^d \\
&= g^{wm} g^{dsw} && \text{as } w_1 = mw \text{ and } w_2 = sw \\
&= g^{w(m+ds)}
\end{aligned}
$$

Correctness

$$
\begin{aligned}
s' &= g^{w_1} Q^{w_2} \\
&= g^{w_1} g^{dw_2} && \text{as } Q = g^d \\
&= g^{wm} g^{dsw} && \text{as } w_1 = mw \text{ and } w_2 = sw \\
&= g^{w(m+ds)} \\
&= g^{t^{-1}(m+ds)} && \text{as } w = t^{-1}
\end{aligned}
$$

Correctness

$$
\begin{aligned}
s' &= g^{w_1} Q^{w_2} \\
&= g^{w_1} g^{dw_2} && \text{as } Q = g^d \\
&= g^{wm} g^{dsw} && \text{as } w_1 = mw \text{ and } w_2 = sw \\
&= g^{w(m+ds)} \\
&= g^{t^{-1}(m+ds)} && \text{as } w = t^{-1} \\
&= g^k && \text{as } t = k^{-1}(m+ds)
\end{aligned}
$$

Correctness

$$
\begin{aligned}
s' &= g^{w_1} Q^{w_2} \\
&= g^{w_1} g^{dw_2} && \text{as } Q = g^d \\
&= g^{wm} g^{dsw} && \text{as } w_1 = mw \text{ and } w_2 = sw \\
&= g^{w(m+ds)} \\
&= g^{t^{-1}(m+ds)} && \text{as } w = t^{-1} \\
&= g^k && \text{as } t = k^{-1}(m+ds) \\
&= s && \text{as } s = g^k.
\end{aligned}
$$

Domain parameter(p, q, g)

- $G = \mathbb{Z}_p^*$ where $p = 92283800153$
- $p - 1 = 2^3 \times 21529 \times 535811$
- $g = 65180204028$, where $O(g) = 535811$

Key Generation

- $d = 14723$.
- $Q \equiv g^d \equiv 3232858927 \mod p$.
- $\mathcal{SK} = 14723$ and $\mathcal{PK} = 3232858927$

Signing$(M, \mathcal{SK})$

1. $k = 9372$
2. $m = \mathcal{H}(M) = 1234567890$
3. $s_1 \equiv g^k \equiv 75248267410 \mod p$
4. $s \equiv s_1 \mod q \equiv 42192 \mod q$
5. $t = k^{-1}(m + ds) \equiv 279309 \mod q$
6. $\sigma = (42192, 279309)$

Signing($M, \mathcal{SK}$)

1. $k = 9372$
2. $m = \mathcal{H}(M) = 1234567890$
3. $s_1 \equiv g^k \equiv 75248267410 \mod p$
4. $s \equiv s_1 \mod q \equiv 42192 \mod q$
5. $t = k^{-1}(m + ds) \equiv 279309 \mod q$
6. $\sigma = (42192, 279309)$

Verification($M, \sigma, \mathcal{PK}$)

1. $m = \mathcal{H}(M) = 1234567890$
2. $w \equiv t^{-1} \equiv 54105 \mod q$
3. $w_1 \equiv mw \equiv 335818 \mod q$
4. $w_2 \equiv sw \equiv 243300 \mod q$
5. $s_1 \equiv (g^{w_1} Q^{w_2}) \equiv 75248267410 \mod p$
6. $s' = s_1 \equiv 42192 \mod q$
7. Check $s' \stackrel{?}{=} s$; If yes Return 1, else Return 0.

Outline for section 5

Public-Key Encryption Schemes

- Digital Signature: {Key Generation, Encryption, Decryption}.
- Key Generation: Probabilistic Polynomial-time (PPT) algorithm.
- Encryption: PPT algorithm.
- Decryption: Deterministic Polynomial-time algorithm.

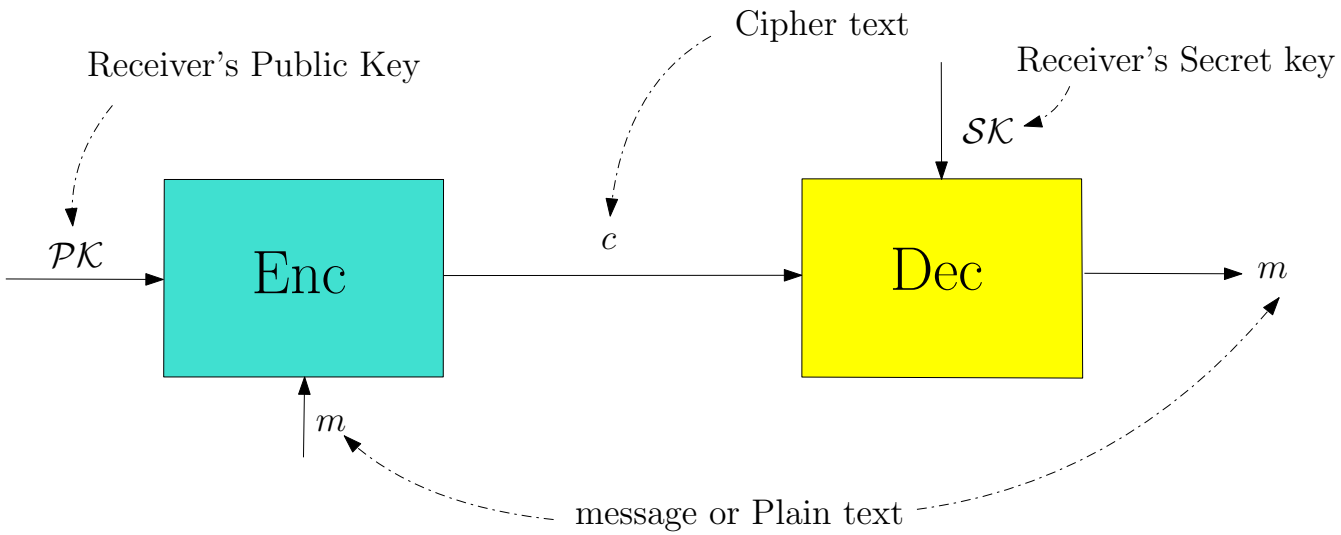


Figure: Public-Key Encryption System

Public-Key Encryption Schemes

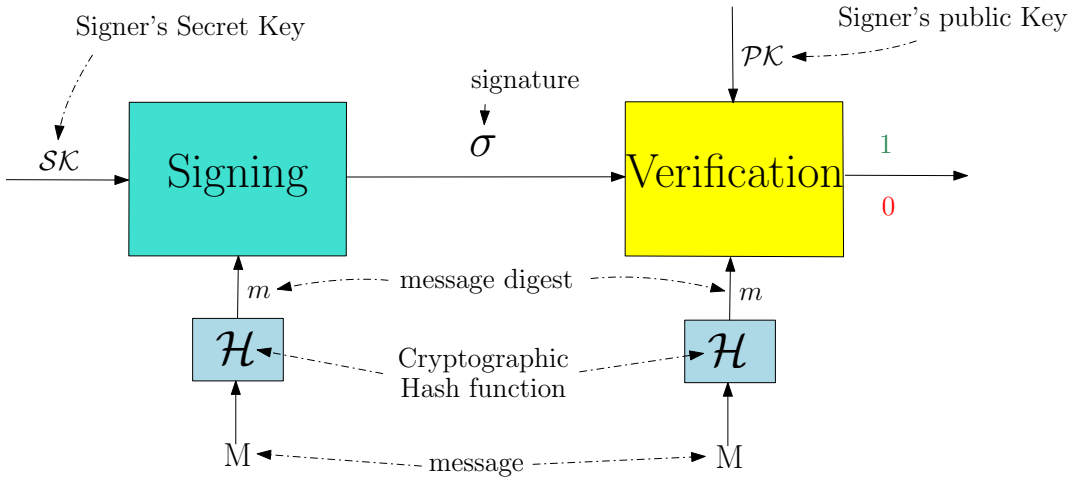


Figure: Digital Signature

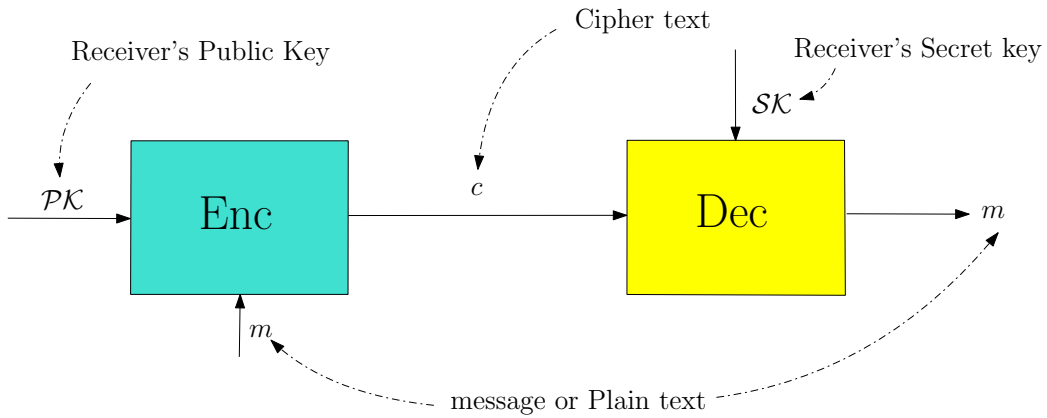


Figure: Digital Signature

Key Generation

1. Let the security parameter be l
2. Choose two primes p and q of bit-length almost l
3. Compute $n = pq$ and $\phi(n) = (p-1)(q-1)$
4. Choose e such that $\gcd(e, \phi(n)) = 1$
5. Compute $d \equiv e^{-1} \mod \phi(n)$
6. $\mathcal{SK} = d$ and $\mathcal{PK} = (n, e)$

RSA Public-Key Encryption Scheme

Encryption($m \in \mathbb{Z}_n^*, \mathcal{PK}$)

1. Compute $c \equiv m^e \mod n$

RSA Public-Key Encryption Scheme

Encryption($m \in \mathbb{Z}_n^*, \mathcal{PK}$)

1. Compute $c \equiv m^e \mod n$

Decryption($c, \mathcal{SK}$)

1. Compute $m = c^d \mod n$

RSA Public-Key Encryption Scheme

Encryption($m \in \mathbb{Z}_n^*, \mathcal{PK}$)

1. Compute $c \equiv m^e \mod n$

Decryption($c, \mathcal{SK}$)

1. Compute $m = c^d \mod n$

Correctness

$$m \equiv c^d \equiv (m^e)^d \equiv m^{ed} \equiv m \mod n,$$

as

$$ed \equiv 1 \mod \phi(n)$$

Key Generation

1. security parameter $l = 18$
2. $p = 241537$ and $q = 382069$
3. $n = pq = 92283800053$
4. $\phi(n) = (241537 - 1)(382069 - 1) = 92283176448$
5. $e = 5$
6. $d \equiv e^{-1} \equiv 55369905869 \mod \phi(n)$
7. $\mathcal{SK} = 55369905869$ and $\mathcal{PK} = (92283800053, 5)$

Encryption$(m, \mathcal{PK})$

1. $m = 1234567890 \in \mathbb{Z}_n^*$.
2. $c \equiv m^e \equiv 40073606699 \mod n$.

Encryption$(m, \mathcal{PK})$

1. $m = 1234567890 \in \mathbb{Z}_n^*$.
2. $c \equiv m^e \equiv 40073606699 \mod n$.

Encryption($m, \mathcal{PK}$)

1. $m = 1234567890 \in \mathbb{Z}_n^*$.
2. $c \equiv m^e \equiv 40073606699 \mod n$.

Verification($c, \mathcal{SK}$)

1. $m = c^d = 1234567890 \in \mathbb{Z}_n^*$.

ElGamal Public-Key Encryption Scheme

Domain parameter

- Let G be a cyclic multiplicative group.
- $O(G) = n$
- $\exists g \in G$ such that $G = \langle g \rangle$ and $O(g) = n$

ElGamal Public-Key Encryption Scheme

Domain parameter

- Let G be a cyclic multiplicative group.
- $O(G) = n$
- $\exists g \in G$ such that $G = \langle g \rangle$ and $O(g) = n$

Key Generation

- Choose $d \in_R \{2, \ldots, n-1\}$
- Compute $Q \equiv g^d$
- $\mathcal{SK} = d$ and $\mathcal{PK} = Q$

Encryption($m, \mathcal{PK}$)

1. Choose $k \in_R \{2, \ldots, n-1\}$
2. Compute $r = g^k$
3. Compute $s = mQ^k$
4. $c = (r, s)$

Encryption($m, \mathcal{PK}$)

1. Choose $k \in_R \{2, \ldots, n-1\}$
2. Compute $r = g^k$
3. Compute $s = mQ^k$
4. $c = (r, s)$

Decryption($c, \mathcal{SK}$)

1. Compute $m = sr^{-d}$

ElGamal Public-Key Encryption Scheme

Encryption($m, \mathcal{PK}$)

1. Choose $k \in_R \{2, \ldots, n-1\}$
2. Compute $r = g^k$
3. Compute $s = mQ^k$
4. $c = (r, s)$

Decryption($c, \mathcal{SK}$)

1. Compute $m = sr^{-d}$

Correctness

$$m = sr^{-d} = mQ^k(g^k)^{-d} = m(g^d)^k(g^k)^{-d} = mg^{kd-kd} = m$$

Domain parameter

- $G = \mathbb{Z}_p^*$ where $p = 92283800099$
- $n = O(G) = 92283800098$
- $g = 19$ and $O(g) = 92283800098$

Domain parameter

- $G = \mathbb{Z}_p^*$ where $p = 92283800099$
- $n = O(G) = 92283800098$
- $g = 19$ and $O(g) = 92283800098$

Key Generation

- $d = 23499347910.$
- $Q \equiv g^d \equiv 66075503407 \mod p.$
- $\mathcal{SK} = 23499347910$ and $\mathcal{PK} = 66075503407$

Encryption($m, \mathcal{SK}$)

1. $k = 9213753243$
2. $m = 1234567890$
3. Compute $r \equiv g^k \equiv 85536409136 \mod p$
4. Compute $s \equiv mQ^k \equiv 9922819653 \mod p$
5. Signature $\sigma = (85536409136, 9922819653)$.

Encryption($m, \mathcal{SK}$)

1. $k = 9213753243$
2. $m = 1234567890$
3. Compute $r \equiv g^k \equiv 85536409136 \mod p$
4. Compute $s \equiv mQ^k \equiv 9922819653 \mod p$
5. Signature $\sigma = (85536409136, 9922819653)$.

Decryption($c, \mathcal{PK}$)

1. Compute $m = sr^{-d} \equiv 1234567890 \mod p$

Outline for section 6

Conclusion

- Basic mathematical tools
- Basic concepts of public-key protocols
- Books:
  - *Cryptography - Theory And Practice*, Douglas Stinson
  - *Cryptography and Network Security Principles and Practices*, William Stallings
  - *Introduction to Cryptography - Principles and Applications*, Hans Delfs, Helmut Knebl
  - *Handbook of Applied Cryptography*, Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone

Questions

Questions

Thank You