

Course Plan

Dr. Odelu Vanga

Computer Science and Engineering
Indian Institute of Information Technology Sri City

odelu.vanga@iiits.in

January 05, 2021

Course Details

Course : Institute Elective
Title : Cryptography
Instructor : Dr. Odelu Vanga

Textbook:

- **Cryptography and Network Security**, Behrouz A Forouzan, Debdeep Mukhopadhyay, McGraw-Hill Education, 2011.
- **Cryptography: Theory and Practice** by Douglas Stinson, 3/e, 2006.

Course Details

Course : Institute Elective
Title : Cryptography
Instructor : Dr. Odelu Vanga

Textbook:

- **Cryptography and Network Security**, Behrouz A Forouzan, Debdeep Mukhopadhyay, McGraw-Hill Education, 2011.
- **Cryptography: Theory and Practice** by Douglas Stinson, 3/e, 2006.

References:

- “Cryptography and Network Security: Principles and Practice”, William Stallings, 6th Edition, Pearson Education, 2014.
- “A course in number theory and cryptography”, Neal Koblitz, Second Edition, Springer.
- “Handbook of Applied Cryptography”, Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, CRC Press.
- “Blockchain Technology Overview”, D. Yaga, P. Mell, N. Roby, and K. Scarfone, NISTIR 8202.
- Classroom Lecture Notes

Evaluation Scheme

Component	Duration	Weightage(%)	Date & Time	Nature of Component
Mid-Sem Exam	–	20%	–	Closed Book
End-Sem Exam	–	30%	–	Closed Book
Scheduled Quiz	–	30%	–	Closed Book
CPQ*	–	10%	–	Closed Book
Term Project	–	10%	–	Open Book

CPQ*: Class Participation Quiz

Term Project Details

- It should submit one page report, includes title and tentative plan work **on/before January 30, 2021**.

Term Project Details

- It should submit one page report, includes title and tentative plan work **on/before January 30, 2021**.
- Submit work implementation plan two pages, include abstract, experiments plan, and summary **on/before March 20, 2021**.

Term Project Details

- It should submit one page report, includes title and tentative plan work **on/before January 30, 2021**.
- Submit work implementation plan two pages, include abstract, experiments plan, and summary **on/before March 20, 2021**.
- Final project report should submit with experimental results on **April 10, 2021**.

Evaluation Scheme

Term Project Details

- It should submit one page report, includes title and tentative plan work **on/before January 30, 2021**.
- Submit work implementation plan two pages, include abstract, experiments plan, and summary **on/before March 20, 2021**.
- Final project report should submit with experimental results on **April 10, 2021**.
- I will announce the **project viva dates** based on the available time slots.

Make-ups and Notices

Make-up policy

- No Make-ups for Term Project.
- Makeup for other components is granted on prior permissions as per institute policy.

Make-ups and Notices

Make-up policy

- No Make-ups for Term Project.
- Makeup for other components is granted on prior permissions as per institute policy.

Consultation and Notices

- Doubt clarification hours - Contact in Google classroom
- Notices/announcements regarding the course will be displayed in Google Classroom

Course Syllabus

Overview of Course Structure

M1: Number Theory Basics

Modular arithmetic, Primes, Euclidean Algorithm, Chinese Remainder Theorem.

M2: Shannon's Theory

Perfect Secrecy, Entropy, Security analysis of Classical ciphers.

M3: Symmetric Key Cryptography

DES, Finite Fields, AES, Security Analysis.

M4: Public Key Cryptography

RSA, ElGamal, Elliptic Curve Cryptography.

M5: Digital Signatures

Hash functions, Digital Signature Algorithm, ElGamal Digital Signature.

M6: Applications

Key Distribution, Diffie-Hellman Key Exchange, Key Management in Distributed Systems.

History

Historical perspective

Before World War II (1940s)

- “**Secret writing**”

- 1900 B.C. – non-standard methods
- Julius Caesar

Historical perspective

Before World War II (1940s)

- “**Secret writing**”
 - 1900 B.C. – non-standard methods
 - Julius Caesar
- **Modern theory starts around the U.S. Civil War (1861-1865)**
 - Playfair

Historical perspective

Before World War II (1940s)

- “**Secret writing**”
 - 1900 B.C. – non-standard methods
 - Julius Caesar
- **Modern theory starts around the U.S. Civil War (1861-1865)**
 - Playfair
- **Extensive use of code books**
 - Telegrams and commercial codes
 - Vernam cipher

World War-I (lasted in 1914 - 1918)

After World War II (1940s)

- **Claude Shannon and Information Theory (1948)**

After World War II (1940s)

- **Claude Shannon and Information Theory (1948)**
- **1974, public interest resumes**
 - Data Encryption Standard (DES, 1977)
 - “New Directions in Cryptography” (1976)
 - Diffie and Hellman’s introduction of Public Key Cryptography

After World War II (1940s)

- **Claude Shannon and Information Theory (1948)**
- **1974, public interest resumes**
 - Data Encryption Standard (DES, 1977)
 - “New Directions in Cryptography” (1976)
 - Diffie and Hellman’s introduction of Public Key Cryptography
 - RSA (Rivest, Shamir, Adelman) (1977)
 - AES - 128 (2001)
 - ECC (1984)

After World War II (1940s)

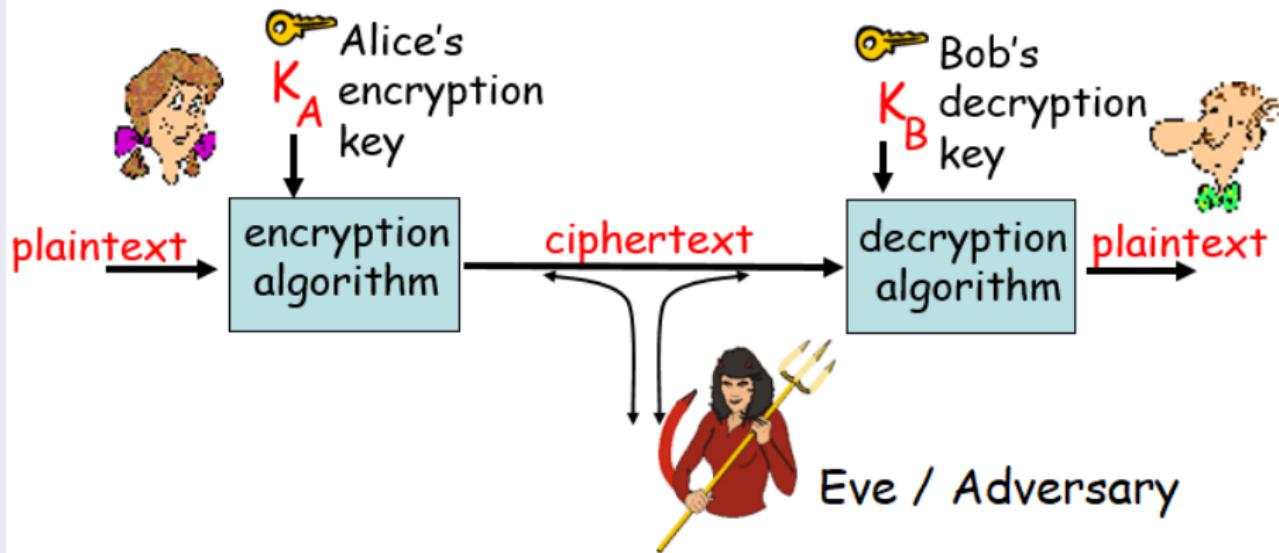
- **Claude Shannon and Information Theory (1948)**
- **1974, public interest resumes**
 - Data Encryption Standard (DES, 1977)
 - “New Directions in Cryptography” (1976)
 - Diffie and Hellman’s introduction of Public Key Cryptography
 - RSA (Rivest, Shamir, Adelman) (1977)
 - AES - 128 (2001)
 - ECC (1984)

Hash Functions

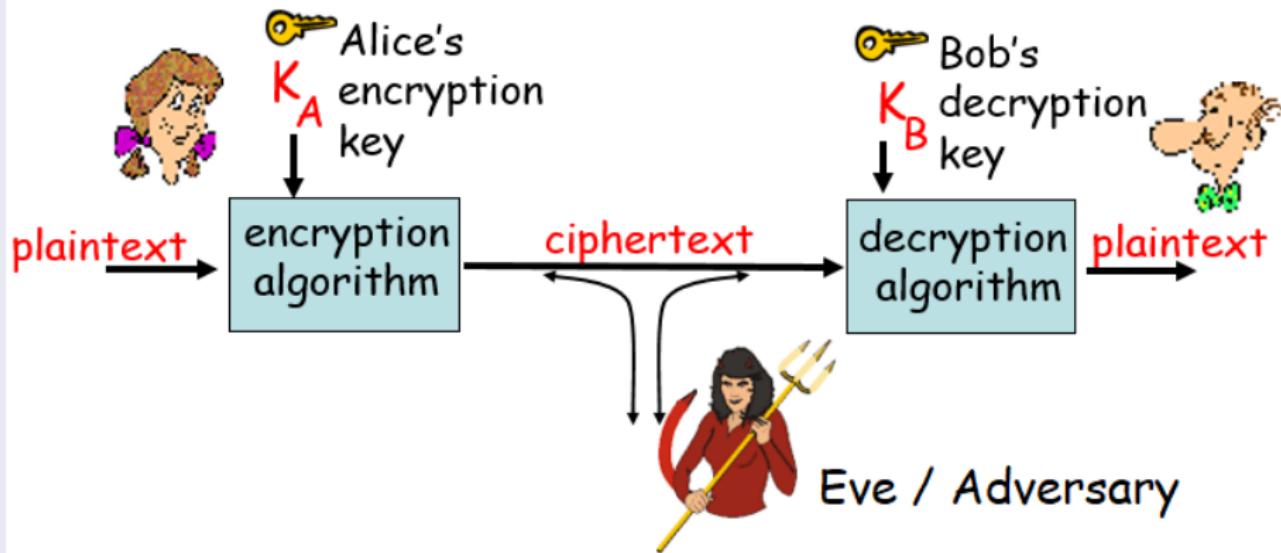
- First design of cryptographic hash function proposed in 1970s
- More proposals emerged in the 1980s

Introduction to cryptography

Message Communication



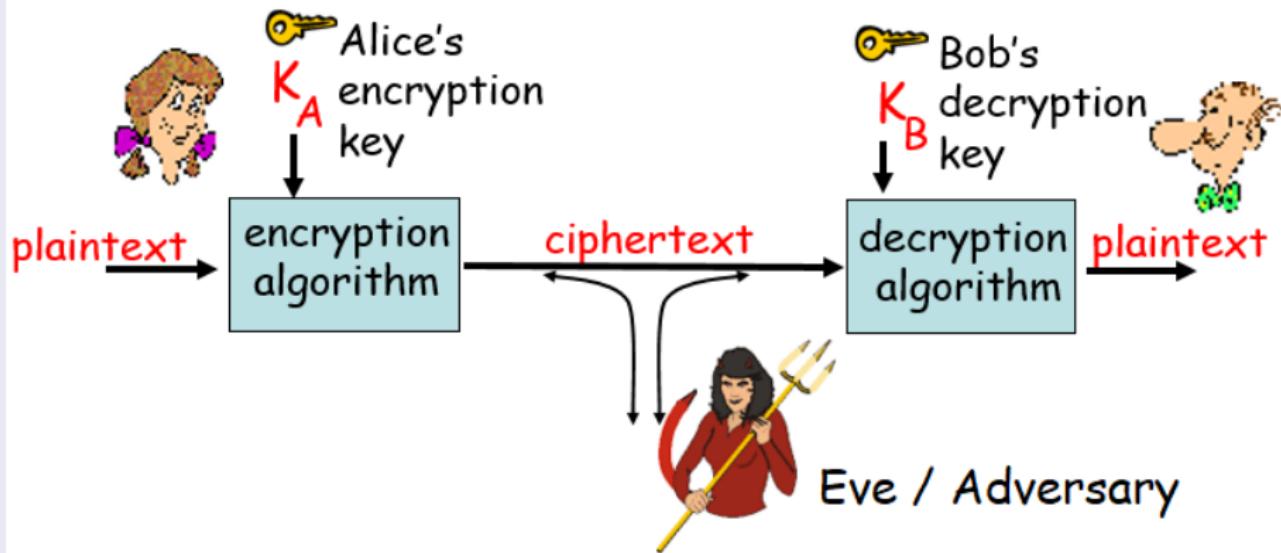
Message Communication



- **Symmetric-key cryptography**

sender, receiver keys are identical, that is, $K_A = K_B$.

Message Communication



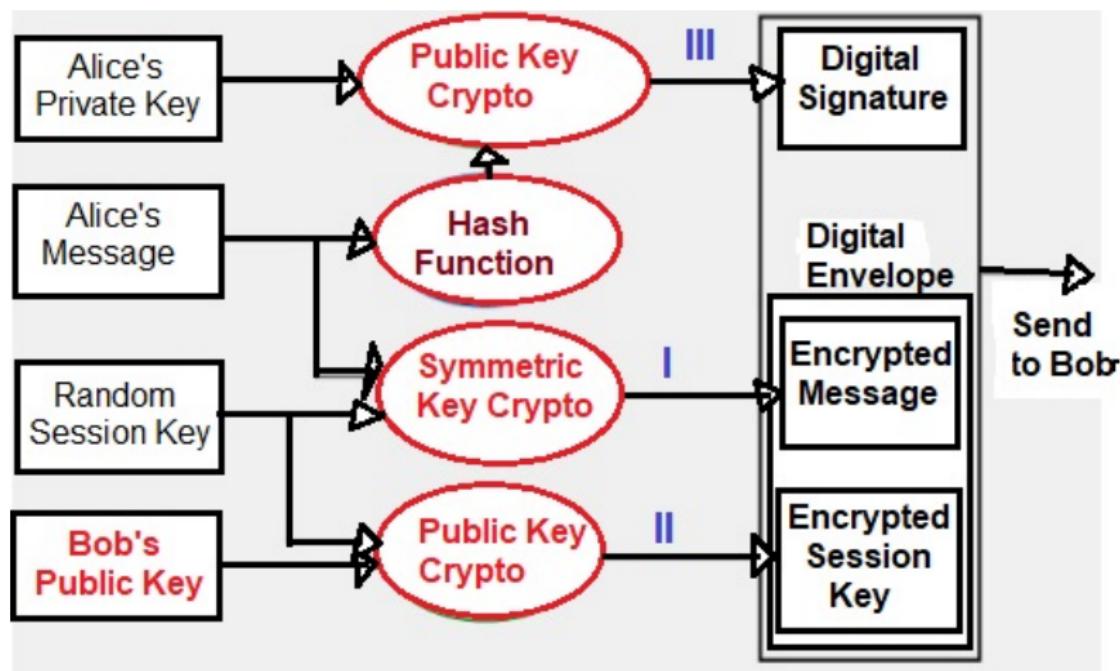
- **Symmetric-key cryptography**

sender, receiver keys are identical, that is, $K_A = K_B$.

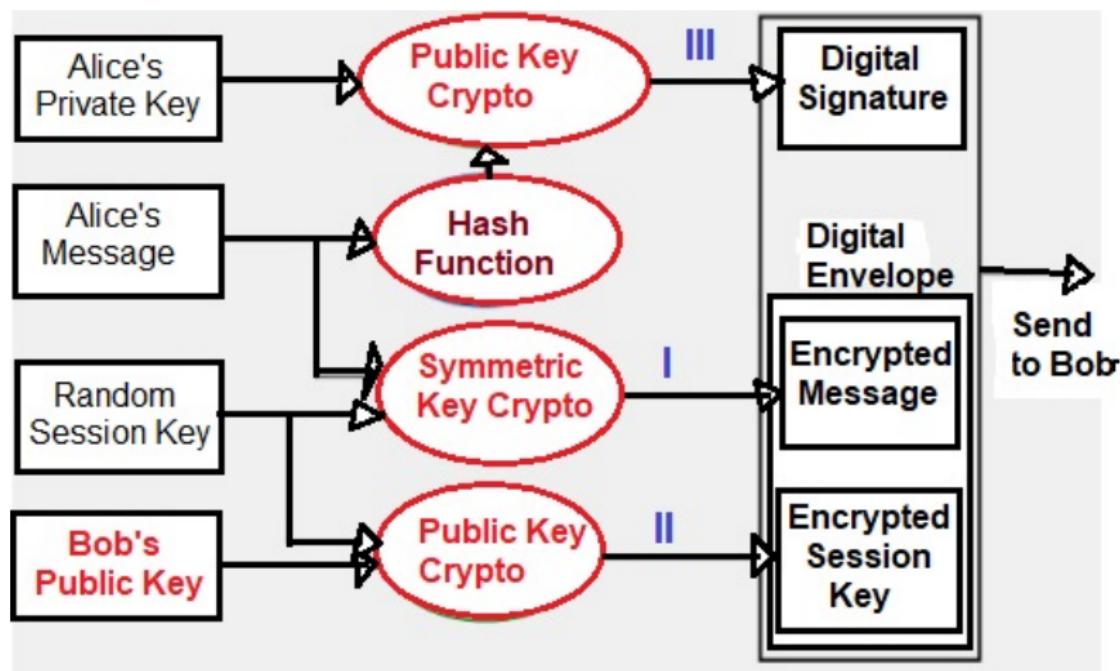
- **Asymmetric-key cryptography**

encryption key (public), decryption key (private), that is, $K_A \neq K_B$.

Goals and Mechanisms

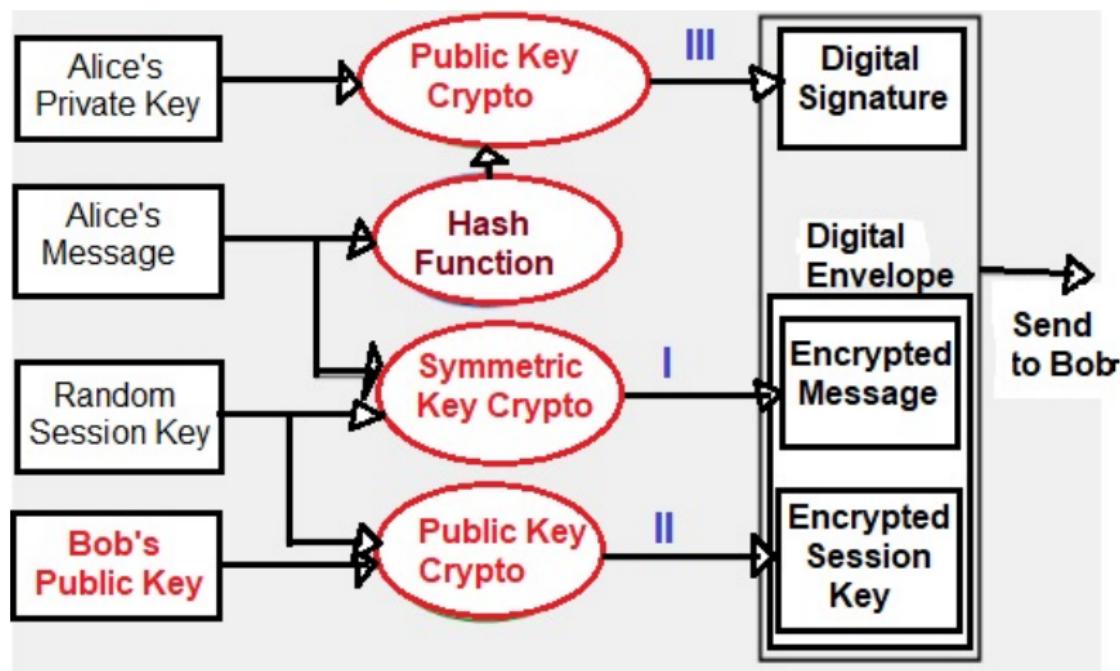


Goals and Mechanisms



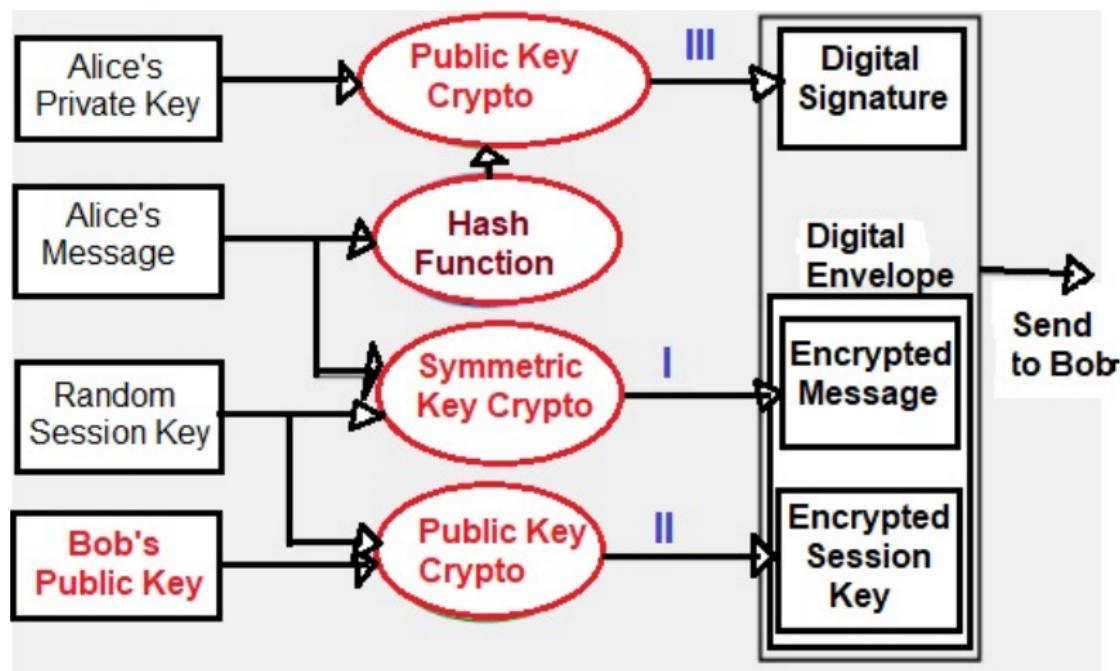
- Confidentiality

Goals and Mechanisms



- Confidentiality
- Integrity

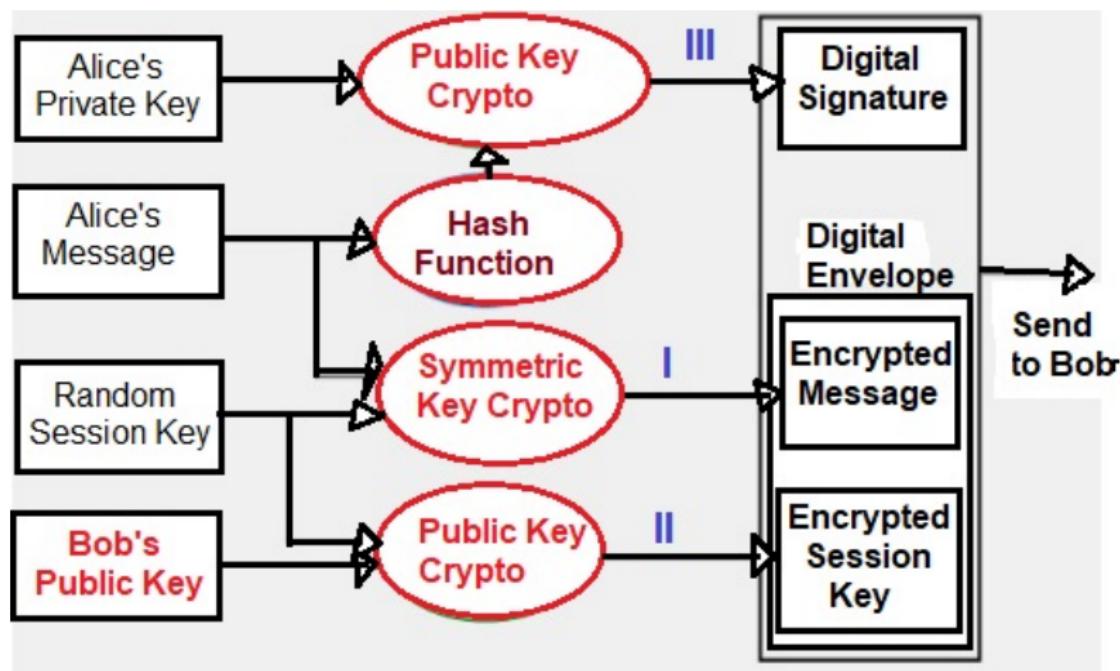
Goals and Mechanisms



- Confidentiality
- Integrity

- Authentication

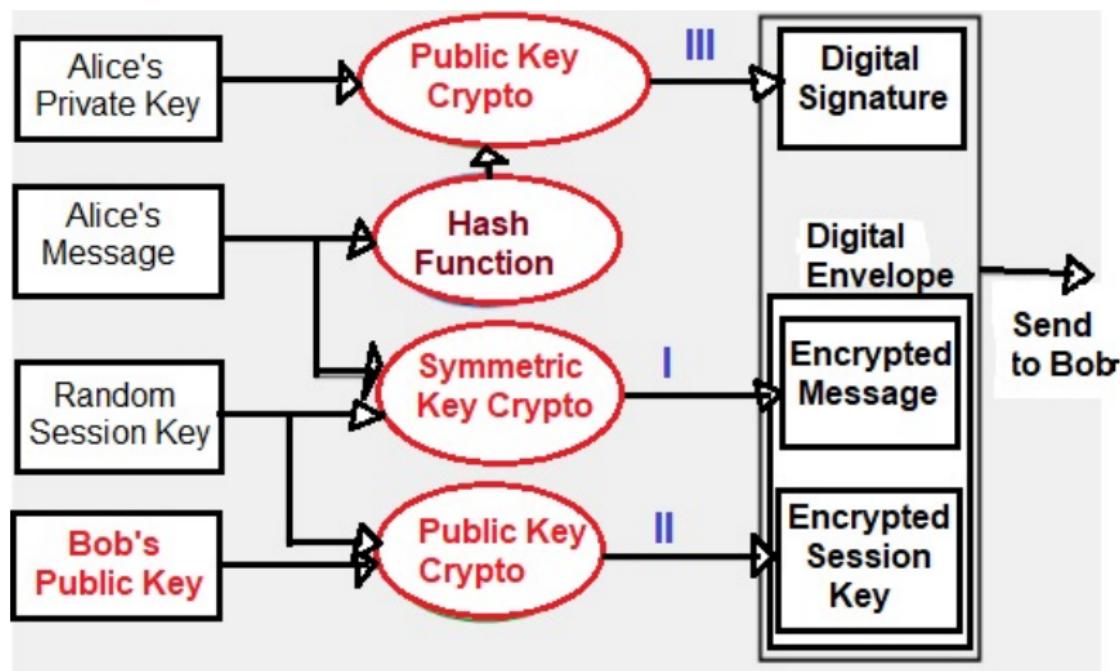
Goals and Mechanisms



- Confidentiality
- Integrity

- Authentication
- Non-repudiation

Goals and Mechanisms



- Confidentiality
- Integrity

- Authentication
- Non-repudiation

Security Notions

Unconditional security

- Given unlimited computational power, it is not possible to break the cipher

Security Notions

Unconditional security

- Given unlimited computational power, it is not possible to break the cipher

Computational security

- Given limited computing resources, breaking cipher is not possible
(e.g., time needed for calculations is greater than age of universe)

Thank You

Euclidean Algorithm

Dr. Odelu Vanga

Computer Science and Engineering
Indian Institute of Information Technology Sri City

odelu.vanga@iiits.in

Today's Objectives

- Modular Arithmetics

Today's Objectives

- Modular Arithmetics
- Euclidean Algorithm

Today's Objectives

- Modular Arithmetics
- Euclidean Algorithm

Modular Arithmetics

Set of Integers

$$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

Modular Arithmetics

Set of Integers

$$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

Note: Integer by integer is not always integer

Example

There is no integer n such that $1/2 = n$

Modular Arithmetics

Set of Integers

$$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

Note: Integer by integer is not always integer

Example

There is no integer n such that $1/2 = n$

Definition

We say that $a (\neq 0)$ divides b , written as $a|b$, if there is an integer k with $b = ka$

Modular Arithmetics

Set of Integers

$$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

Note: Integer by integer is not always integer

Example

There is no integer n such that $1/2 = n$

Definition

We say that $a (\neq 0)$ divides b , written as $a|b$, if there is an integer k with $b = ka$

- Examples: $2|4$, $(-7)|7$, and $6|0$

Basic Properties of Divisibility

- If $a|b$, then $a|bc$ for any c
- If $a|b$ and $b|c$, then $a|c$
- If $a|b$ and $a|c$, then $a|(xb + yc)$ for any x and y
- If $a|b$ and $b|a$, then $a = \pm b$
- If $a|b$, and $a, b > 0$, then $a \leq b$
- For any $m \neq 0$, $a|b$ is equivalent to $(ma)|(mb)$

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

- Furthermore, $r = 0$ if and only if $b|a$

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

- Furthermore, $r = 0$ if and only if $b|a$

Definition (Common Divisor)

If $d|a$ and $d|b$, then d is a common divisor of a and b

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

- Furthermore, $r = 0$ if and only if $b|a$

Definition (Common Divisor)

If $d|a$ and $d|b$, then d is a common divisor of a and b

- Largest one is called greatest common divisor

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

- Furthermore, $r = 0$ if and only if $b|a$

Definition (Common Divisor)

If $d|a$ and $d|b$, then d is a common divisor of a and b

- Largest one is called greatest common divisor

Example

- Positive divisors of 30 are 1, 2, 3, 5, 6, 10, 15, 30

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

- Furthermore, $r = 0$ if and only if $b|a$

Definition (Common Divisor)

If $d|a$ and $d|b$, then d is a common divisor of a and b

- Largest one is called greatest common divisor

Example

- Positive divisors of 30 are 1, 2, 3, 5, 6, 10, 15, 30
- Positive divisors of 42 are 1, 2, 3, 6, 7, 14, 21, 42

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

- Furthermore, $r = 0$ if and only if $b|a$

Definition (Common Divisor)

If $d|a$ and $d|b$, then d is a common divisor of a and b

- Largest one is called greatest common divisor

Example

- Positive divisors of 30 are 1, 2, 3, 5, 6, 10, 15, 30
- Positive divisors of 42 are 1, 2, 3, 6, 7, 14, 21, 42
- Common (positive) divisors are 1, 2, 3, 6
- $GCD(30, 42) = 6$

Relatively Prime

If $GCD(a, b) = 1$, we say a and b are relatively prime

Relatively Prime

If $GCD(a, b) = 1$, we say a and b are relatively prime

Example

- 7 and 12 are relatively prime

Relatively Prime

If $GCD(a, b) = 1$, we say a and b are relatively prime

Example

- 7 and 12 are relatively prime
- But, 8 and 32 are not relatively prime

Relatively Prime

If $GCD(a, b) = 1$, we say a and b are relatively prime

Example

- 7 and 12 are relatively prime
- But, 8 and 32 are not relatively prime
- 11 and 13 are relatively prime

Basic facts about greatest common divisors

- If $m > 0$, then $\text{GCD}(ma, mb) = m \times \text{GCD}(a, b)$

Basic facts about greatest common divisors

- If $m > 0$, then $\text{GCD}(ma, mb) = m \times \text{GCD}(a, b)$
- If $d > 0$ divides both a and b , then
 $\text{GCD}(a/d, b/d) = \text{GCD}(a, b)/d$

Basic facts about greatest common divisors

- If $m > 0$, then $\text{GCD}(ma, mb) = m \times \text{GCD}(a, b)$
- If $d > 0$ divides both a and b , then
$$\text{GCD}(a/d, b/d) = \text{GCD}(a, b)/d$$
- If both a and b relatively prime to m , then so is ab

Basic facts about greatest common divisors

- If $m > 0$, then $\text{GCD}(ma, mb) = m \times \text{GCD}(a, b)$
- If $d > 0$ divides both a and b , then
$$\text{GCD}(a/d, b/d) = \text{GCD}(a, b)/d$$
- If both a and b relatively prime to m , then so is ab
- For any integer x , $\text{GCD}(a, b) = \text{GCD}(a, b + ax)$

Basic facts about greatest common divisors

- If $m > 0$, then $\text{GCD}(ma, mb) = m \times \text{GCD}(a, b)$
- If $d > 0$ divides both a and b , then
$$\text{GCD}(a/d, b/d) = \text{GCD}(a, b)/d$$
- If both a and b relatively prime to m , then so is ab
- For any integer x , $\text{GCD}(a, b) = \text{GCD}(a, b + ax)$
- If $c|ab$ and b, c are relatively prime, then $c|a$

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of **zero** is obtained

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of **zero** is obtained

Algorithm (q_i - quotient and r_i - remainder)

$$a = q_1 b + r_1$$

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of **zero** is obtained

Algorithm (q_i - quotient and r_i - remainder)

$$\begin{array}{rcl} a & = q_1 b + r_1 \\ b & = q_2 r_1 + r_2 \end{array}$$

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of **zero** is obtained

Algorithm (q_i - quotient and r_i - remainder)

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \end{aligned}$$

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of **zero** is obtained

Algorithm (q_i - quotient and r_i - remainder)

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-1} &= q_k r_k + r_k + 1 \end{aligned}$$

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of **zero** is obtained

Algorithm (q_i - quotient and r_i - remainder)

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-1} &= q_k r_k + r_k + 1 \\ r_k &= q_{k+1} r_{k+1} \end{aligned}$$

Then $d = GCD(a, b)$ is equal to the last nonzero remainder, r_{k+1}

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of **zero** is obtained

Algorithm (q_i - quotient and r_i - remainder)

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-1} &= q_k r_k + r_k + 1 \\ r_k &= q_{k+1} r_{k+1} \end{aligned}$$

Then $d = GCD(a, b)$ is equal to the last nonzero remainder, r_{k+1}

- **Linear Combination:** There exist integers x and y such that $d = ax + by$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, $\text{GCD}(42, 36) = 6$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, $\text{GCD}(42, 36) = 6$

Linear Combination of (30, 42)

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, $\text{GCD}(42, 36) = 6$

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, $\text{GCD}(42, 36) = 6$

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$

$$6 = 30 - 2 \times 12$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, $\text{GCD}(42, 36) = 6$

We have to find x and y such that $6 = 30x + 42y$

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$

$$6 = 30 - 2 \times 12$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, $\text{GCD}(42, 36) = 6$

We have to find x and y such that $6 = 30x + 42y$

$$6 = 30 - 2 \times 12$$

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$

$$6 = 30 - 2 \times 12$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, $\text{GCD}(42, 36) = 6$

We have to find x and y such that $6 = 30x + 42y$

$$6 = 30 - 2 \times 12$$

$$6 = 30 - 2 \times (42 - 1 \times 30)$$

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$

$$6 = 30 - 2 \times 12$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, $\text{GCD}(42, 36) = 6$

We have to find x and y such that $6 = 30x + 42y$

$$6 = 30 - 2 \times 12$$

$$6 = 30 - 2 \times (42 - 1 \times 30)$$

$$\text{Hence, } 6 = 30 \times 3 - 42 \times 2$$

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$

$$6 = 30 - 2 \times 12$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, $\text{GCD}(42, 36) = 6$

We have to find x and y such that $6 = 30x + 42y$

$$6 = 30 - 2 \times 12$$

$$6 = 30 - 2 \times (42 - 1 \times 30)$$

$$\text{Hence, } 6 = 30 \times 3 - 42 \times 2$$

That is, $x = 3$ and $y = -2$

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$

$$6 = 30 - 2 \times 12$$

Thank You

Residue Classes

Dr. Odelu Vanga

Computer Science and Engineering
Indian Institute of Information Technology Sri City

odelu.vanga@iiits.in

Today's Objectives

- Residue Classes

Today's Objectives

- Residue Classes
- Finding Inverse Modulo m

Today's Objectives

- Residue Classes
- Finding Inverse Modulo m
- General Caesar Cipher

Today's Objectives

- Residue Classes
- Finding Inverse Modulo m
- General Caesar Cipher
- Affine Cipher

Residue Classes

Definition

If m is a positive integer and m divides $(b - a)$, then we say that

- a and b are congruent modulo m
- we write $a \equiv b \pmod{m}$

Residue Classes

Definition

If m is a positive integer and m divides $(b - a)$, then we say that

- a and b are congruent modulo m
- we write $a \equiv b \pmod{m}$

Examples:

- $3 \equiv 9 \pmod{6}$, since 6 divides $9 - 3 = 6$

Residue Classes

Definition

If m is a positive integer and m divides $(b - a)$, then we say that

- a and b are congruent modulo m
- we write $a \equiv b \pmod{m}$

Examples:

- $3 \equiv 9 \pmod{6}$, since 6 divides $9 - 3 = 6$
- $-2 \equiv 28 \pmod{5}$, since 5 divides $28 - (-2) = 30$

Residue Classes

Definition

If m is a positive integer and m divides $(b - a)$, then we say that

- a and b are congruent modulo m
- we write $a \equiv b \pmod{m}$

Examples:

- $3 \equiv 9 \pmod{6}$, since 6 divides $9 - 3 = 6$
- $-2 \equiv 28 \pmod{5}$, since 5 divides $28 - (-2) = 30$
- $0 \equiv -666 \pmod{3}$, since 3 divides $-666 - 0 = -666$

Residue Classes

Definition

If m is a positive integer and m divides $(b - a)$, then we say that

- a and b are congruent modulo m
- we write $a \equiv b \pmod{m}$

Examples:

- $3 \equiv 9 \pmod{6}$, since 6 divides $9 - 3 = 6$
- $-2 \equiv 28 \pmod{5}$, since 5 divides $28 - (-2) = 30$
- $0 \equiv -666 \pmod{3}$, since 3 divides $-666 - 0 = -666$

If m does not divide $b - a$, we say a and b are not congruent mod m , and write $a \not\equiv b \pmod{m}$

Residue Classes

Definition

If m is a positive integer and m divides $(b - a)$, then we say that

- a and b are congruent modulo m
- we write $a \equiv b \pmod{m}$

Examples:

- $3 \equiv 9 \pmod{6}$, since 6 divides $9 - 3 = 6$
- $-2 \equiv 28 \pmod{5}$, since 5 divides $28 - (-2) = 30$
- $0 \equiv -666 \pmod{3}$, since 3 divides $-666 - 0 = -666$

If m does not divide $b - a$, we say a and b are not congruent mod m , and write $a \not\equiv b \pmod{m}$

- $2 \not\equiv 7 \pmod{3}$, because 3 does not divide $7 - 2 = 5$

Residue Classes

- $a = q_1 m + r_1$ and $b = q_2 m + r_2$,
where $0 \leq r_1 \leq m - 1$ and $0 \leq r_2 \leq m - 1$.
- $a \equiv b \pmod{m}$ if and only if $r_1 = r_2$.

Residue Classes

- $a = q_1 m + r_1$ and $b = q_2 m + r_2$,
where $0 \leq r_1 \leq m - 1$ and $0 \leq r_2 \leq m - 1$.
- $a \equiv b \pmod{m}$ if and only if $r_1 = r_2$.
- $r_1 = a \pmod{m}$ denotes the remainder.

Residue Classes

- $a = q_1 m + r_1$ and $b = q_2 m + r_2$,
where $0 \leq r_1 \leq m - 1$ and $0 \leq r_2 \leq m - 1$.
- $a \equiv b \pmod{m}$ if and only if $r_1 = r_2$.
- $r_1 = a \pmod{m}$ denotes the remainder.
- Thus, $a \equiv b \pmod{m}$ if and only if $a \pmod{m} = b \pmod{m}$.

Residue Classes

- $a = q_1 m + r_1$ and $b = q_2 m + r_2$,
where $0 \leq r_1 \leq m - 1$ and $0 \leq r_2 \leq m - 1$.
- $a \equiv b \pmod{m}$ if and only if $r_1 = r_2$.
- $r_1 = a \pmod{m}$ denotes the remainder.
- Thus, $a \equiv b \pmod{m}$ if and only if $a \pmod{m} = b \pmod{m}$.

Definition (Residue Class)

If a is an integer and $a \equiv b \pmod{m}$, we say that b is a residue of $a \pmod{m}$.

Residue Classes

- $a = q_1 m + r_1$ and $b = q_2 m + r_2$,
where $0 \leq r_1 \leq m - 1$ and $0 \leq r_2 \leq m - 1$.
- $a \equiv b \pmod{m}$ if and only if $r_1 = r_2$.
- $r_1 = a \pmod{m}$ denotes the remainder.
- Thus, $a \equiv b \pmod{m}$ if and only if $a \pmod{m} = b \pmod{m}$.

Definition (Residue Class)

If a is an integer and $a \equiv b \pmod{m}$, we say that b is a residue of $a \pmod{m}$.

- The residue class of a modulo m , denoted \bar{a} , is the collection of all integers congruent to a modulo m .

Residue Classes

- $a = q_1 m + r_1$ and $b = q_2 m + r_2$,
where $0 \leq r_1 \leq m - 1$ and $0 \leq r_2 \leq m - 1$.
- $a \equiv b \pmod{m}$ if and only if $r_1 = r_2$.
- $r_1 = a \pmod{m}$ denotes the remainder.
- Thus, $a \equiv b \pmod{m}$ if and only if $a \pmod{m} = b \pmod{m}$.

Definition (Residue Class)

If a is an integer and $a \equiv b \pmod{m}$, we say that b is a residue of $a \pmod{m}$.

- The residue class of a modulo m , denoted \bar{a} , is the collection of all integers congruent to a modulo m .
- Observe that $\bar{a} = \{a + km, k \in \mathbb{Z}\}$.

Set of Residue Class

- The residue class of a modulo m , denoted \bar{a} , is the collection of all integers congruent to a modulo m .
- Observe that $\bar{a} = \{a + km, k \in \mathbb{Z}\}$.

Set of Residue Class

- The residue class of a modulo m , denoted \bar{a} , is the collection of all integers congruent to a modulo m .
- Observe that $\bar{a} = \{a + km, k \in \mathbb{Z}\}$.

Set of residue class $\{0, 1, 2, \dots, m - 1\}$ modulo m is denoted by \mathbb{Z}_m , that is,

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

- Addition and Multiplication works exactly like real addition and multiplication, except reduce modulo m .

Set of Residue Class

- The residue class of a modulo m , denoted \bar{a} , is the collection of all integers congruent to a modulo m .
- Observe that $\bar{a} = \{a + km, k \in \mathbb{Z}\}$.

Set of residue class $\{0, 1, 2, \dots, m - 1\}$ modulo m is denoted by \mathbb{Z}_m , that is,

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

- Addition and Multiplication works exactly like real addition and multiplication, except reduce modulo m .
- $11 \times 13 = 143$ in \mathbb{Z}_{16} , and reduce it to modulo 16:

Set of Residue Class

- The residue class of a modulo m , denoted \bar{a} , is the collection of all integers congruent to a modulo m .
- Observe that $\bar{a} = \{a + km, k \in \mathbb{Z}\}$.

Set of residue class $\{0, 1, 2, \dots, m - 1\}$ modulo m is denoted by \mathbb{Z}_m , that is,

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

- Addition and Multiplication works exactly like real addition and multiplication, except reduce modulo m .
- $11 \times 13 = 143$ in \mathbb{Z}_{16} , and reduce it to modulo 16:
 $143 = 8 \times 16 + 15$, so $143 \pmod{16} = 15 \in \mathbb{Z}_{16}$

Definition (Inverse of an element)

Suppose $a \in \mathbb{Z}_m$. The multiplicative inverse of a is an element $a^{-1} \in \mathbb{Z}_m$ such that $aa^{-1} = a^{-1}a = 1 \pmod{m}$

Finding Inverse Modulo m

Theorem (Multiplicative Inverse Modulo m)

a and m relatively primes if and only if a^{-1} modulo m exists

Finding Inverse Modulo m

Theorem (Multiplicative Inverse Modulo m)

a and m relatively primes if and only if a^{-1} modulo m exists

Proof.

Suppose a and m are relatively prime

Then, $GCD(a, m) = 1$

Finding Inverse Modulo m

Theorem (Multiplicative Inverse Modulo m)

a and m relatively primes if and only if a^{-1} modulo m exists

Proof.

Suppose a and m are relatively prime

Then, $GCD(a, m) = 1$

There exists x and y such that $1 = ax + my$

Now apply modulo m , we get $1 = (ax + 0) \pmod{m}$

That is, $1 = ax \pmod{m}$

Means, there exists x such that $ax = 1 \pmod{m}$

Therefore, x is inverse of a modulo m



Example: Finding Inverse Modulo m

Find multiplicative inverse of $a = 8$ modulo $m = 11$

Example: Finding Inverse Modulo m

Find multiplicative inverse of $a = 8$ modulo $m = 11$

Finding $8^{-1} \pmod{11}$ using Euclidean Algorithm

$$m = qa + r$$

$$a = q_1r + r_1$$

- $11 = (1) \times 8 + 3$
- $8 = (2) \times 3 + 2$
- $3 = (1) \times 2 + 1$
- $2 = (2) \times 1 + 0$

Example: Finding Inverse Modulo m

Find multiplicative inverse of $a = 8$ modulo $m = 11$

Finding $8^{-1} \pmod{11}$ using Euclidean Algorithm

$$m = qa + r$$

$$a = q_1r + r_1$$

- $11 = (1) \times 8 + 3$
- $8 = (2) \times 3 + 2$
- $3 = (1) \times 2 + 1$
- $2 = (2) \times 1 + 0$

Rewrite

- $3 = 11 - (1) \times 8$
- $2 = 8 - (2) \times 3$
- $1 = 3 - (1) \times 2$

Example: Finding Inverse Modulo m

Find multiplicative inverse of $a = 8$ modulo $m = 11$

Finding $8^{-1} \pmod{11}$ using Euclidean Algorithm

$$m = qa + r$$

Reverse the process:

$$a = q_1r + r_1$$

- $11 = (1) \times 8 + 3$
- $8 = (2) \times 3 + 2$
- $3 = (1) \times 2 + 1$
- $2 = (2) \times 1 + 0$

Rewrite

- $3 = 11 - (1) \times 8$
- $2 = 8 - (2) \times 3$
- $1 = 3 - (1) \times 2$

Example: Finding Inverse Modulo m

Find multiplicative inverse of $a = 8$ modulo $m = 11$

Finding $8^{-1} \pmod{11}$ using Euclidean Algorithm

$$m = qa + r$$

$$a = q_1r + r_1$$

Reverse the process:

find $1 = 8x + 11y$ form

- $11 = (1) \times 8 + 3$
- $8 = (2) \times 3 + 2$
- $3 = (1) \times 2 + 1$
- $2 = (2) \times 1 + 0$

Rewrite

- $3 = 11 - (1) \times 8$
- $2 = 8 - (2) \times 3$
- $1 = 3 - (1) \times 2$

Example: Finding Inverse Modulo m

Find multiplicative inverse of $a = 8$ modulo $m = 11$

Finding $8^{-1} \pmod{11}$ using Euclidean Algorithm

$$m = qa + r$$

$$a = q_1r + r_1$$

Reverse the process:

find $1 = 8x + 11y$ form

- $11 = (1) \times 8 + 3$
- $8 = (2) \times 3 + 2$
- $3 = (1) \times 2 + 1$
- $2 = (2) \times 1 + 0$

Rewrite

- $3 = 11 - (1) \times 8$
- $2 = 8 - (2) \times 3$
- $1 = 3 - (1) \times 2$

$$\begin{aligned} 1 &= 3 - (1) \times 2 \\ &= 3 - (1) \times [8 - (2) \times 3] \\ &= (-1) \times 8 + (3) \times 3 \\ &= (-1) \times 8 + (3) \times [11 - (1) \times 8] \\ &= (-4) \times 8 + (3) \times 11 \end{aligned}$$

$$x = -4 \pmod{11} = 7 = 8^{-1} \pmod{11}$$

Finding Inverse

Find Inverse of 7 modulo 26

Remainder Form

$$26 = (3) \times 7 + 5$$

$$7 = (1) \times 5 + 2$$

$$5 = (2) \times 2 + 1$$

$$2 = (2) \times 1 + 0$$

Rewrite

$$5 = 26 - (3) \times 7$$

$$2 = 7 - (1) \times 5$$

$$1 = 5 - (2) \times 2$$

Finding Inverse

Find Inverse of 7 modulo 26

Remainder Form

$$26 = (3) \times 7 + 5$$

$$7 = (1) \times 5 + 2$$

$$5 = (2) \times 2 + 1$$

$$2 = (2) \times 1 + 0$$

Rewrite

$$5 = 26 - (3) \times 7$$

$$2 = 7 - (1) \times 5$$

$$1 = 5 - (2) \times 2$$

Reverse Process

$$1 = 5 - (2) \times 2$$

$$1 = 5 - (2) \times [7 - (1) \times 5]$$

$$1 = (-2) \times 7 + (3) \times 5$$

$$1 = (-2) \times 7 + (3) \times [26 - (3) \times 7]$$

$$1 = (-11) \times 7 + (3) \times 26$$

$$x = -11 \pmod{26} = 15 = 7^{-1} \pmod{26}$$

Finding Inverse

Find Inverse of 7 modulo 26

Remainder Form

$$26 = (3) \times 7 + 5$$

$$7 = (1) \times 5 + 2$$

$$5 = (2) \times 2 + 1$$

$$2 = (2) \times 1 + 0$$

Rewrite

$$5 = 26 - (3) \times 7$$

$$2 = 7 - (1) \times 5$$

$$1 = 5 - (2) \times 2$$

Reverse Process

$$1 = 5 - (2) \times 2$$

$$1 = 5 - (2) \times [7 - (1) \times 5]$$

$$1 = (-2) \times 7 + (3) \times 5$$

$$1 = (-2) \times 7 + (3) \times [26 - (3) \times 7]$$

$$1 = (-11) \times 7 + (3) \times 26$$

$$x = -11 \pmod{26} = 15 = 7^{-1} \pmod{26}$$

Finding Inverse

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

Finding Inverse

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Finding Inverse

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

Finding Inverse

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$
- $1 = 5x + 26y$
where $x = -5$ and $y = 1$

Rewrite

- $1 = 26 - 5 \times 5$

Finding Inverse

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Finding Inverse

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

General Caesar Cipher

- Assign numerical value from 0 - 25 to each letter of plaintext alphabet $a - z$, respectively.

General Caesar Cipher

- Assign numerical value from 0 - 25 to each letter of plaintext alphabet $a - z$, respectively.
- $\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_{26} = \{0, 1, 2, \dots, 25\}$

General Caesar Cipher

- Assign numerical value from 0 - 25 to each letter of plaintext alphabet $a - z$, respectively.
- $\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_{26} = \{0, 1, 2, \dots, 25\}$
 Z_{26} - set of remainders when divide by 26
- Encryption function $E_k : \mathcal{P} \rightarrow \mathcal{C}$ and
decryption function $D_k : \mathcal{C} \rightarrow \mathcal{P}$, where $k \in \mathcal{K}$, defined as follows:

General Caesar Cipher

- Assign numerical value from 0 - 25 to each letter of plaintext alphabet $a - z$, respectively.
- $\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_{26} = \{0, 1, 2, \dots, 25\}$
 Z_{26} - set of remainders when divide by 26
- Encryption function $E_k : \mathcal{P} \rightarrow \mathcal{C}$ and decryption function $D_k : \mathcal{C} \rightarrow \mathcal{P}$, where $k \in \mathcal{K}$, defined as follows:

$$C = E_k(m) = (m + k) \pmod{26}$$

General Caesar Cipher

- Assign numerical value from 0 - 25 to each letter of plaintext alphabet $a - z$, respectively.
- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26} = \{0, 1, 2, \dots, 25\}$
 \mathbb{Z}_{26} - set of remainders when divide by 26
- Encryption function $E_k : \mathcal{P} \rightarrow \mathcal{C}$ and decryption function $D_k : \mathcal{C} \rightarrow \mathcal{P}$, where $k \in \mathcal{K}$, defined as follows:

$$C = E_k(m) = (m + k) \pmod{26}$$

$$m = D_k(C) = (C - k) \pmod{26}$$

General Caesar Cipher

- Assign numerical value from 0 - 25 to each letter of plaintext alphabet $a - z$, respectively.
- $\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_{26} = \{0, 1, 2, \dots, 25\}$
 Z_{26} - set of remainders when divide by 26
- Encryption function $E_k : \mathcal{P} \rightarrow \mathcal{C}$ and decryption function $D_k : \mathcal{C} \rightarrow \mathcal{P}$, where $k \in \mathcal{K}$, defined as follows:

$$C = E_k(m) = (m + k) \pmod{26}$$

$$m = D_k(C) = (C - k) \pmod{26}$$

where $m, C \in Z_{26}$

General Caesar Cipher

- Assign numerical value from 0 - 25 to each letter of plaintext alphabet $a - z$, respectively.
- $\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_{26} = \{0, 1, 2, \dots, 25\}$
 Z_{26} - set of remainders when divide by 26
- Encryption function $E_k : \mathcal{P} \rightarrow \mathcal{C}$ and decryption function $D_k : \mathcal{C} \rightarrow \mathcal{P}$, where $k \in \mathcal{K}$, defined as follows:

$$\begin{aligned} C &= E_k(m) = (m + k) \pmod{26} \\ m &= D_k(C) = (C - k) \pmod{26} \end{aligned}$$

where $m, C \in Z_{26}$

Note that, if key $k = 3$, it is simply a Caesar cipher.

General Caesar Cipher

Example

Find the Caesar cipher of a simple message $m = \text{"crypto"}$ with the key $k = 3$

General Caesar Cipher

Example

Find the Caesar cipher of a simple message $m = \text{"crypto"}$ with the key $k = 3$

- Assume that $m = m_1 m_2 \dots m_n$ the plaintext message with n letters m_1 to m_n

General Caesar Cipher

Example

Find the Caesar cipher of a simple message $m = \text{"crypto"}$ with the key $k = 3$

- Assume that $m = m_1 m_2 \dots m_n$ the plaintext message with n letters m_1 to m_n
- Then $m_1 = c, m_2 = r, m_3 = y, m_4 = p, m_5 = t, m_6 = o$

General Caesar Cipher

Example

Find the Caesar cipher of a simple message $m = \text{"crypto"}$ with the key $k = 3$

- Assume that $m = m_1 m_2 \dots m_n$ the plaintext message with n letters m_1 to m_n
- Then $m_1 = c, m_2 = r, m_3 = y, m_4 = p, m_5 = t, m_6 = o$
- Suppose the corresponding ciphertext letters are C_1 to C_n

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$$m = \text{"crypto"} \text{ and } C_i = E_k(m_i) = (m_i + k) \pmod{26}$$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26}$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26}$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$$m = \text{"crypto"} \text{ and } C_i = E_k(m_i) = (m_i + k) \pmod{26}$$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26}$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26}$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$$m = \text{"crypto"} \text{ and } C_i = E_k(m_i) = (m_i + k) \pmod{26}$$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26} = 20 = U$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26} = 20 = U$$

$$C_3 = E_k(m_3) = (24 + 3) \pmod{26}$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26} = 20 = U$$

$$C_3 = E_k(m_3) = (24 + 3) \pmod{26} = 27 \pmod{26}$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26} = 20 = U$$

$$C_3 = E_k(m_3) = (24 + 3) \pmod{26} = 27 \pmod{26} = 1 = B$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26} = 20 = U$$

$$C_3 = E_k(m_3) = (24 + 3) \pmod{26} = 27 \pmod{26} = 1 = B$$

$$C_4 = E_k(m_4) = (15 + 3) \pmod{26}$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26} = 20 = U$$

$$C_3 = E_k(m_3) = (24 + 3) \pmod{26} = 27 \pmod{26} = 1 = B$$

$$C_4 = E_k(m_4) = (15 + 3) \pmod{26} = 18 \pmod{26}$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26} = 20 = U$$

$$C_3 = E_k(m_3) = (24 + 3) \pmod{26} = 27 \pmod{26} = 1 = B$$

$$C_4 = E_k(m_4) = (15 + 3) \pmod{26} = 18 \pmod{26} = 18 = S$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26} = 20 = U$$

$$C_3 = E_k(m_3) = (24 + 3) \pmod{26} = 27 \pmod{26} = 1 = B$$

$$C_4 = E_k(m_4) = (15 + 3) \pmod{26} = 18 \pmod{26} = 18 = S$$

$$C_5 = E_k(m_5) = (19 + 3) \pmod{26}$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26} = 20 = U$$

$$C_3 = E_k(m_3) = (24 + 3) \pmod{26} = 27 \pmod{26} = 1 = B$$

$$C_4 = E_k(m_4) = (15 + 3) \pmod{26} = 18 \pmod{26} = 18 = S$$

$$C_5 = E_k(m_5) = (19 + 3) \pmod{26} = 22 \pmod{26} = 22$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26} = 20 = U$$

$$C_3 = E_k(m_3) = (24 + 3) \pmod{26} = 27 \pmod{26} = 1 = B$$

$$C_4 = E_k(m_4) = (15 + 3) \pmod{26} = 18 \pmod{26} = 18 = S$$

$$C_5 = E_k(m_5) = (19 + 3) \pmod{26} = 22 \pmod{26} = 22 = W$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26} = 20 = U$$

$$C_3 = E_k(m_3) = (24 + 3) \pmod{26} = 27 \pmod{26} = 1 = B$$

$$C_4 = E_k(m_4) = (15 + 3) \pmod{26} = 18 \pmod{26} = 18 = S$$

$$C_5 = E_k(m_5) = (19 + 3) \pmod{26} = 22 \pmod{26} = 22 = W$$

$$C_6 = E_k(m_6) = (14 + 3) \pmod{26}$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26} = 20 = U$$

$$C_3 = E_k(m_3) = (24 + 3) \pmod{26} = 27 \pmod{26} = 1 \pmod{26} = 1 = B$$

$$C_4 = E_k(m_4) = (15 + 3) \pmod{26} = 18 \pmod{26} = 18 = S$$

$$C_5 = E_k(m_5) = (19 + 3) \pmod{26} = 22 \pmod{26} = 22 = W$$

$$C_6 = E_k(m_6) = (14 + 3) \pmod{26} = 17 \pmod{26}$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26} = 20 = U$$

$$C_3 = E_k(m_3) = (24 + 3) \pmod{26} = 27 \pmod{26} = 1 = B$$

$$C_4 = E_k(m_4) = (15 + 3) \pmod{26} = 18 \pmod{26} = 18 = S$$

$$C_5 = E_k(m_5) = (19 + 3) \pmod{26} = 22 \pmod{26} = 22 = W$$

$$C_6 = E_k(m_6) = (14 + 3) \pmod{26} = 17 \pmod{26} = 17 = R$$

General Caesar Cipher

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		

Encryption algorithm works as follows:

$m = \text{"crypto"}$ and $C_i = E_k(m_i) = (m_i + k) \pmod{26}$

$$C_1 = E_k(m_1) = (2 + 3) \pmod{26} = 5 \pmod{26} = 5 = F$$

$$C_2 = E_k(m_2) = (17 + 3) \pmod{26} = 20 \pmod{26} = 20 = U$$

$$C_3 = E_k(m_3) = (24 + 3) \pmod{26} = 27 \pmod{26} = 1 \pmod{26} = 1 = B$$

$$C_4 = E_k(m_4) = (15 + 3) \pmod{26} = 18 \pmod{26} = 18 = S$$

$$C_5 = E_k(m_5) = (19 + 3) \pmod{26} = 22 \pmod{26} = 22 = W$$

$$C_6 = E_k(m_6) = (14 + 3) \pmod{26} = 17 \pmod{26} = 17 = R$$

The ciphertext C is "FUBSWR", that is, $E_3(\text{crypto}) = FUBSWR$

Affine Cipher

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, and

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : GCD(a, 26) = 1\}$$

$$C = E_k(m) = (am + b) \pmod{26}$$

$$m = D_k(C) = a^{-1}(C - b) \pmod{26}$$

where $m, C \in \mathbb{Z}_{26}$

Affine Cipher

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, and

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \text{GCD}(a, 26) = 1\}$$

$$C = E_k(m) = (am + b) \pmod{26}$$

$$m = D_k(C) = a^{-1}(C - b) \pmod{26}$$

where $m, C \in \mathbb{Z}_{26}$

Correctness proof:

$$D_k(E_k(m)) = D_k(am + b) \pmod{26}$$

Affine Cipher

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, and

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \text{GCD}(a, 26) = 1\}$$

$$C = E_k(m) = (am + b) \pmod{26}$$

$$m = D_k(C) = a^{-1}(C - b) \pmod{26}$$

where $m, C \in \mathbb{Z}_{26}$

Correctness proof:

$$\begin{aligned} D_k(E_k(m)) &= D_k(am + b) \pmod{26} \\ &= a^{-1}((am + b) - b) \pmod{26} \end{aligned}$$

Affine Cipher

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, and

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \text{GCD}(a, 26) = 1\}$$

$$C = E_k(m) = (am + b) \pmod{26}$$

$$m = D_k(C) = a^{-1}(C - b) \pmod{26}$$

where $m, C \in \mathbb{Z}_{26}$

Correctness proof:

$$\begin{aligned} D_k(E_k(m)) &= D_k(am + b) \pmod{26} \\ &= a^{-1}((am + b) - b) \pmod{26} \\ &= a^{-1}(am) \pmod{26} \\ &= (a^{-1}a)m \pmod{26} \\ &= m \pmod{26} \\ &= m \end{aligned}$$

Affine Cipher: Correctness

Suppose $k = (7, 3)$, then

- $C = E_k(m) = 7m + 3 \pmod{26}$

Affine Cipher: Correctness

Suppose $k = (7, 3)$, then

- $C = E_k(m) = 7m + 3 \pmod{26}$

Remainder Form

$$26 = (3) \times 7 + 5$$

$$7 = (1) \times 5 + 2$$

$$5 = (2) \times 2 + 1$$

$$2 = (2) \times 1 + 0$$

Affine Cipher: Correctness

Suppose $k = (7, 3)$, then

- $C = E_k(m) = 7m + 3 \pmod{26}$

Remainder Form

$$26 = (3) \times 7 + 5$$

$$7 = (1) \times 5 + 2$$

$$5 = (2) \times 2 + 1$$

$$2 = (2) \times 1 + 0$$

Reverse Process

$$1 = 5 - (2) \times 2$$

$$1 = 5 - (2) \times [7 - (1) \times 5]$$

$$1 = (-2) \times 7 + (3) \times 5$$

$$1 = (-2) \times 7 + (3) \times [26 - (3) \times 7]$$

$$1 = (-11) \times 7 + (3) \times 26$$

$$x = -11 \pmod{26} = 15$$

Affine Cipher: Correctness

Suppose $k = (7, 3)$, then

- $C = E_k(m) = 7m + 3 \pmod{26}$

Remainder Form

$$26 = (3) \times 7 + 5$$

$$7 = (1) \times 5 + 2$$

$$5 = (2) \times 2 + 1$$

$$2 = (2) \times 1 + 0$$

Reverse Process

$$1 = 5 - (2) \times 2$$

$$1 = 5 - (2) \times [7 - (1) \times 5]$$

$$1 = (-2) \times 7 + (3) \times 5$$

$$1 = (-2) \times 7 + (3) \times [26 - (3) \times 7]$$

$$1 = (-11) \times 7 + (3) \times 26$$

$$x = -11 \pmod{26} = 15$$

Correctness

$$D_k(C) = 15(C - 3) \pmod{26}$$

Affine Cipher: Correctness

Suppose $k = (7, 3)$, then

- $C = E_k(m) = 7m + 3 \pmod{26}$

Remainder Form

$$26 = (3) \times 7 + 5$$

$$7 = (1) \times 5 + 2$$

$$5 = (2) \times 2 + 1$$

$$2 = (2) \times 1 + 0$$

Reverse Process

$$1 = 5 - (2) \times 2$$

$$1 = 5 - (2) \times [7 - (1) \times 5]$$

$$1 = (-2) \times 7 + (3) \times 5$$

$$1 = (-2) \times 7 + (3) \times [26 - (3) \times 7]$$

$$1 = (-11) \times 7 + (3) \times 26$$

$$x = -11 \pmod{26} = 15$$

Correctness

$$\begin{aligned} D_k(C) &= 15(C - 3) \pmod{26} \\ &= 15([7m + 3] - 3) \pmod{26} \end{aligned}$$

Affine Cipher: Correctness

Suppose $k = (7, 3)$, then

- $C = E_k(m) = 7m + 3 \pmod{26}$

Remainder Form

$$26 = (3) \times 7 + 5$$

$$7 = (1) \times 5 + 2$$

$$5 = (2) \times 2 + 1$$

$$2 = (2) \times 1 + 0$$

Reverse Process

$$1 = 5 - (2) \times 2$$

$$1 = 5 - (2) \times [7 - (1) \times 5]$$

$$1 = (-2) \times 7 + (3) \times 5$$

$$1 = (-2) \times 7 + (3) \times [26 - (3) \times 7]$$

$$1 = (-11) \times 7 + (3) \times 26$$

$$x = -11 \pmod{26} = 15$$

Correctness

$$\begin{aligned} D_k(C) &= 15(C - 3) \pmod{26} \\ &= 15([7m + 3] - 3) \pmod{26} \\ &= 105m \pmod{26} \end{aligned}$$

Affine Cipher: Correctness

Suppose $k = (7, 3)$, then

- $C = E_k(m) = 7m + 3 \pmod{26}$

Remainder Form

$$26 = (3) \times 7 + 5$$

$$7 = (1) \times 5 + 2$$

$$5 = (2) \times 2 + 1$$

$$2 = (2) \times 1 + 0$$

Reverse Process

$$1 = 5 - (2) \times 2$$

$$1 = 5 - (2) \times [7 - (1) \times 5]$$

$$1 = (-2) \times 7 + (3) \times 5$$

$$1 = (-2) \times 7 + (3) \times [26 - (3) \times 7]$$

$$1 = (-11) \times 7 + (3) \times 26$$

$$x = -11 \pmod{26} = 15$$

Correctness

$$\begin{aligned} D_k(C) &= 15(C - 3) \pmod{26} \\ &= 15([7m + 3] - 3) \pmod{26} \\ &= 105m \pmod{26} \\ &= m \end{aligned}$$

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : “*crypto*”
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : “crypto”
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext		c	r	y	p	t	o
-----------	--	---	---	---	---	---	---

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : “crypto”
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2					

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : “crypto”
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17				

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext m	c	r	y	p	t	o
	2	17	24			

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15		

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext m	c	r	y	p	t	o
	2	17	24	15	19	14

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$						

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12					

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext m	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87				

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext m	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122			

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77		

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$						

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12					

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9				

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18			

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18	25		

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18	25	19	

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18	25	19	20

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18	25	19	20
ciphertext	M					

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18	25	19	20
ciphertext	M	J				

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18	25	19	20
ciphertext	M	J	S			

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18	25	19	20
ciphertext	M	J	S	Z		

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18	25	19	20
ciphertext	M	J	S	Z	T	

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18	25	19	20
ciphertext	M	J	S	Z	T	U

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18	25	19	20
ciphertext	M	J	S	Z	T	U

That is, $E_K(\text{crypto}) = MJSZTU$.

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18	25	19	20
ciphertext	M	J	S	Z	T	U

That is, $E_K(\text{crypto}) = \text{MJSZTU}$.

- The decryption function is $m = D_k(C) = 5^{-1}(C - 2) \pmod{26}$

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18	25	19	20
ciphertext	M	J	S	Z	T	U

That is, $E_K(\text{crypto}) = \text{MJSZTU}$.

- The decryption function is $m = D_k(C) = 5^{-1}(C - 2) \pmod{26}$
- We have to find the value of $5^{-1} \pmod{26}$

Affine Cipher: Encryption

Find the Affine cipher for given

- the plaintext message m : "crypto"
- key $k = (a, b) = (5, 2)$, then $C = E_k(m) = 5m + 2 \pmod{26}$

Encryption

plaintext	c	r	y	p	t	o
m	2	17	24	15	19	14
$5m + 2$	12	87	122	77	97	72
$(5m + 2) \pmod{26}$	12	9	18	25	19	20
ciphertext	M	J	S	Z	T	U

That is, $E_K(\text{crypto}) = \text{MJSZTU}$.

- The decryption function is $m = D_k(C) = 5^{-1}(C - 2) \pmod{26}$
- We have to find the value of $5^{-1} \pmod{26}$

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$
- $1 = 5x + 26y$
where $x = -5$ and $y = 1$

Rewrite

- $1 = 26 - 5 \times 5$

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210					

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147				

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336			

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483		

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	378

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	378
$21(C - 2) \pmod{26}$	2					

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	378
$21(C - 2) \pmod{26}$	2	17				

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	378
$21(C - 2) \pmod{26}$	2	17	24			

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	378
$21(C - 2) \pmod{26}$	2	17	24	15		

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	378
$21(C - 2) \pmod{26}$	2	17	24	15	19	

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	378
$21(C - 2) \pmod{26}$	2	17	24	15	19	14

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	378
$21(C - 2) \pmod{26}$	2	17	24	15	19	14
plaintext	c					

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	378
$21(C - 2) \pmod{26}$	2	17	24	15	19	14
plaintext	c	r				

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	378
$21(C - 2) \pmod{26}$	2	17	24	15	19	14
plaintext	c	r	y			

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	378
$21(C - 2) \pmod{26}$	2	17	24	15	19	14
plaintext	c	r	y	p		

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	378
$21(C - 2) \pmod{26}$	2	17	24	15	19	14
plaintext	c	r	y	p	t	

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	378
$21(C - 2) \pmod{26}$	2	17	24	15	19	14
plaintext	c	r	y	p	t	o

Affine Cipher: Decryption

Finding $5^{-1} \pmod{26}$ using Euclidean Algorithm

- $26 = 5 \times 5 + 1$
- $5 = 5 \times 1 + 0$

Rewrite

- $1 = 26 - 5 \times 5$

- $1 = 5x + 26y$
where $x = -5$ and $y = 1$
- $1 = 5x \pmod{26}$, that is,
 $x = 5^{-1} = -5 \pmod{26} = 21$

Decryption

ciphertext	M	J	S	Z	T	U
C	12	9	18	25	19	20
$21(C - 2)$	210	147	336	483	357	378
$21(C - 2) \pmod{26}$	2	17	24	15	19	14
plaintext	c	r	y	p	t	o

Remark: If $a = 1$, the Affine cipher becomes simply a Caesar cipher, that is, $C = E_K(m) = x + b \pmod{26}$.

Thank You

Primes

Dr. Odelu Vanga

Computer Science and Engineering
Indian Institute of Information Technology
Sri City, India

Prime Numbers

Prime numbers: divisors of 1 and itself

- They cannot be written as a product of other numbers

Prime: 2,3,5,7

Not primes: 4,6,8,9,10

List of prime number less than 200 is:

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
61	67	71	73	79	83	89	97	101	103	107	109	113				
127	131	137	139	149	151	157	163	167	173	179						
181	191	193	197	199												

Prime Factorisation

Factorization: $n=a \times b \times c$

Note that factoring a number is relatively hard compared to multiplying the factors together to generate the number

The **prime factorisation** of a number **n** is **unique**
(a product of primes)

$$91 = 7 \times 13$$

$$3600 = 2^4 \times 3^2 \times 5^2$$

Relatively Prime Numbers & GCD

Two numbers a, b are **relatively prime** if the **common divisor is 1**

- Eg. 8 and 15 are relatively prime

since factors of 8 are 1,2,4,8 and

15 are 1,3,5,15 and

1 is the only common factor

- eg. $300 = 2^1 \times 3^1 \times 5^2$ and $18 = 2^1 \times 3^2$

$$\text{GCD}(18, 300) = 2^1 \times 3^1 \times 5^0 = 6$$

Fermat's Little Theorem

Let p is prime and a is a positive integer not divisible by p , then

$$a^{p-1} \bmod p = 1$$

Eg. $p=7$, $a=4$, $4^{7-1} \bmod 7 = 1$

- In the above case, p divides exactly into $a^p - a$.

Fermat's primality test is a necessary, but not sufficient test for primality.

- For example, let $a = 2$ and $n = 341$, then a and n are relatively prime and 341 divides exactly into $2^{341} - 2$.
- However, $341 = 11 \times 31$, so it is a composite number.
- Thus, 341 is a Fermat **pseudoprime** to the base 2

Euler Totient Function $\phi(n)$

Number of relatively primes to n from 0 to $(n-1)$.

- when doing arithmetic modulo n
- **Complete set of residues:** $\{0 \dots n-1\}$
- **E.g.** for $n=10$,
- Complete set of residues: $\{0,1,2,3,4,5,6,7,8,9\}$
- Reduced set of residues: $\{1,3,7,9\}$

Euler Totient Function $\phi(n)$:

- **number of elements** in reduced set of residues of n
- **$\phi(10) = 4$**

Euler Totient Function $\phi(n)$

To compute $\phi(n)$, we need to count number of elements to be excluded

In general, it needs prime factorization.

We know

- for p (p prime) $\phi(p) = p-1$
- for $p \cdot q$ (p, q prime) $\phi(p \cdot q) = (p-1)(q-1)$

E.g.

- $\phi(37) = 36$
- $\phi(21) = (3-1) \times (7-1) = 2 \times 6 = 12$

Euler's Theorem

A generalisation of Fermat's Theorem

$$a^{\phi(n)} \pmod{n} = 1$$

where $\gcd(a, n) = 1$

E.g.

- $a=3; n=10; \phi(10)=4;$

Hence $3^4 = 81 = 1 \pmod{10}$

- $a=2; n=11; \phi(11)=10;$

Hence, $2^{10} = 1024 = 1 \pmod{11}$

Primality Testing

Many cryptographic algorithms needs large prime numbers

Traditionally, **sieve** using **trial division**

- divide by all numbers (primes) in turn less than the square root of the number
- only works for small numbers

Statistical primality tests

- all prime numbers satisfy property
- But, some composite numbers, called **pseudo-primes**, also satisfy the property, with a low probability.

Prime is in P: Deterministic polynomial algorithm - 2002.

Miller Rabin Algorithm

A test based on Fermat's Theorem

TEST (n) is:

1. Find biggest k , $k > 0$, so that $(n-1) = 2^k q$
2. Select a random integer a , $1 < a < n-1$
3. if $a^q \text{ mod } n = 1$ then return ("maybe prime");
4. for $j=0$ to $k-1$ do
 - 5. if $(a^{2^j q} \text{ mod } n = n-1)$
then return(" maybe prime ")
6. return ("composite")

TEST (n) is:

1. Find biggest k , $k > 0$, so that $(n-1) = 2^k q$
2. Select a random integer a , $1 < a < n-1$
3. if $a^q \text{ mod } n = 1$ then return ("maybe prime");
4. for $j = 0$ to $k-1$ do
 5. if $(a^{2^j q} \text{ mod } n = n-1)$
 then return(" maybe prime ")
6. return ("composite")

Probabilistic Considerations

- If Miller-Rabin returns “composite” the number is definitely not prime
- Otherwise is a prime or a pseudo-prime
- Chance it detects a pseudo-prime is $< \frac{1}{4}$
- Hence if repeat test with different random a then chance n is prime after t tests is:
 - $\Pr(n \text{ prime after } t \text{ tests}) = 1 - 4^{-t}$
 - eg. for $t=10$ this probability is > 0.99999

Prime Distribution

- There are infinite prime numbers
 - Euclid’s proof
- Prime number theorem states that
 - primes near n occur roughly every $(\ln n)$ integers
- Since can immediately ignore evens and multiples of 5, in practice only need test $0 . 4 \ln(n)$ numbers before locate a prime around n
 - Note this is only the “average” sometimes primes are close together, at other times are quite far apart

THANK YOU

Chinese Remainder Theorem (Applications)

DR. ODELU VANGA

COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF INFORMATION TECHNOLOGY
SRI CITY, INDIA

Linear Congruences, Inverses

A congruence of the form $\underline{ax \equiv b \pmod{m}}$ is called a *linear congruence*.

- To *solve* the congruence is to find the x 's that satisfy it.

An *inverse of a , modulo m* is any integer a' such that $\underline{a'a \equiv 1 \pmod{m}}$.

- If we can find such an a' , notice that we can then solve $\underline{ax \equiv b}$ by multiplying through by it.
- Implies $\underline{a'ax \equiv a'b}$, thus $\underline{1 \cdot x \equiv a'b}$, thus $\underline{x \equiv a'b \pmod{m}}$.

Theorem: If $\underline{\gcd(a,m)=1}$ and $\underline{m>1}$, then a has a unique (modulo m) inverse a' .

- Proof: By theorem 1, $\exists s, t: sa+tm = 1$, so $\underline{sa+tm \equiv 1 \pmod{m}}$.

Since $\underline{tm \equiv 0 \pmod{m}}$, $\underline{sa \equiv 1 \pmod{m}}$. Thus s is an inverse of a (mod m).

From the result, if $\underline{ra \equiv sa \equiv 1}$ then $\underline{r \equiv s}$.

Thus this inverse is unique mod m . (All inverses of a are in the same congruence class as s .)

Note: Linear congruences are the basis to perform arithmetic with large integers.

Example:

Find an inverse of 4 modulo 9

Since $\text{gcd}(4, 9) = 1$, we know that there is an inverse of 4, modulo 9.

Using the Euclidean algorithm to find the greatest common divisor:

$$9 = 2 \times 4 + 1$$

Rewrite:

$$9 - 2 \times 4 = 1$$

So, -2 is an inverse of 4 module 9

We have: $-2 \times 4 = -8$. And $-8 \bmod 9 = 1$.

What are the solutions of the linear congruence $4x \equiv 5 \pmod{9}$? X

Since we know that -2 is an inverse for $4 \pmod{9}$,
we can multiply both sides of the linear congruence:

$$\underline{-2} \times \underline{4x} \equiv \underline{-2} \times \underline{5} \pmod{9}$$

Since $-8 \equiv 1 \pmod{9}$ and $-10 \equiv 8 \pmod{9}$,
it follows that if x is a solution, then $\underline{x} \equiv \underline{-10} \equiv \underline{8} \pmod{9}$.

$$x = (a^{-1})^b \pmod{m^b}$$

a^{-1} mod m exists

$$xa = (0)^b \pmod{m^b}$$

We now have $4x \equiv 4 \times 8 \equiv 5 \pmod{9}$ which shows that all such x satisfy the congruence.

So, solutions x such that $x \equiv 8 \pmod{9}$, namely, $8, 17, 26, \dots$, and $-1, -10$, etc.

Puzzle

There are certain things whose number is unknown.

- When divided by 3, the remainder is 2;
- when divided by 5, the remainder is 3; and
- when divided by 7, the remainder is 2.

What is the number of things?

What's x such that:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}?$$



Chinese Remainder Theorem

Theorem: (Chinese remainder theorem.)

Let $m_1, \dots, m_n > 0$ be relatively prime.

Then the system of equations $x \equiv \underline{a_i} \pmod{m_i}$ (for $i=1$ to n)

has a unique solution modulo $m = \underline{m_1 \cdot \dots \cdot m_n}$.

Proof: Let $\underline{M_i = m/m_i}$.

Since $\gcd(m_i, M_i) = 1$, $\exists y_i$ such that $\underline{y_i M_i \equiv 1 \pmod{m_i}}$.

Now let $x = \sum_i a_i y_i M_i$.

Since $m_j | M_k$ for $k \neq i$, $M_k \equiv 0 \pmod{m_i}$, so $\underline{x \equiv a_i y_i M_i \equiv a_i \pmod{m_i}}$.

Thus, the congruences hold.

(Uniqueness is an exercise.)

Computer Arithmetic with Large Integers

By Chinese Remainder Theorem, an integer a where $0 \leq a < m = \prod m_i$, $\gcd(m_i, m_{j \neq i}) = 1$,
can be represented by a 's residues mod m_i :

$$(a \bmod m_1, a \bmod m_2, \dots, a \bmod m_n)$$


Implicitly, consider the set of equations $x \equiv a_i \pmod{m_i}$. With $a_i = a \bmod m_i$.
By the CRT, unique $x \equiv a \pmod{m}$, with $m = \prod m_i$ is a solution.



How to represent uniquely all integers less than 12 by pairs, where the first component is the remainder of the integer upon division by 3 and the second component is the remainder of the integer upon division by 4?

Finding the remainder of each integer divide by 3 and 4, we obtain:

$$a = (a \bmod 3, a \bmod 4) \text{ e.g. } 5 = ((5 \bmod 3), (5 \bmod 4)) = (2, 1)$$

$$0=(0,0);$$

$$1=(1,1);$$

$$2=(2,2);$$

$$3=(\cancel{0},\cancel{3});$$

$$4=(1,0);$$

$$5=(2,1);$$

$$6=(0,2);$$

$$7=(\cancel{1},\cancel{3});$$

$$8=(2,0);$$

$$9=(0,1);$$

$$10=(1,2);$$

$$11=(\cancel{2},\cancel{3})$$

Note we have the right “number of pairs”; one for each number up to $4 \times 3 - 1$.

Computer Arithmetic with Large Integers

To perform arithmetic upon large integers represented in this way,

- Simply perform operations on these separate residues!
 - Each of these might be done in a single machine operation.
 - The operations may be easily parallelized on a vector machine.
- Works so long as the desired result $< m$.

Suppose we can perform operation with integers less than 100 can be done easily; we can restrict ourselves to integers less than 100, if we represent the integers using their remainders modulo pairwise relatively prime integers less than 100; e.g., 99, 98, 97, 95.

By the Chinese remainder theorem, any number up to

$$99 \times 98 \times 97 \times 95 = 89,403,930$$

can be represented uniquely by its remainders when divided by these four moduli.

For example, the number 123684 can be represented as

$$(123684 \bmod 99; 123684 \bmod 98; 123684 \bmod 97; 123684 \bmod 95) = (33, 8, 9, 89)$$

413456 can be represented as

$$(413456 \bmod 99; 413456 \bmod 98; 413456 \bmod 97; 413456 \bmod 95) = (32, 92, 42, 16)$$

To perform a sum we only have to sum the residues:

$$\begin{aligned}& (33, 8, 9, 89) + (32, 92, 42, 16) \\&= (65 \bmod 99, 100 \bmod 98, 51 \bmod 97, 105 \bmod 95) \\&= (65, 2, 51, 10)\end{aligned}$$

To find the sum we just have to solve the system of linear congruences:

$$\begin{aligned}x &\equiv 65 \pmod{99} \\x &\equiv 2 \pmod{98} \\x &\equiv 51 \pmod{97} \\x &\equiv 10 \pmod{95}\end{aligned}$$


Solution: **537140 = 123684 + 413456**

“Bigger” Example

For example, the following numbers are relatively prime:

$$\begin{aligned}m_1 &= 2^{25}-1 = 33,554,431 = 31 \cdot 601 \cdot 1,801 & \checkmark \\m_2 &= 2^{27}-1 = 134,217,727 = 7 \cdot 73 \cdot 262,657 & \checkmark \\m_3 &= 2^{28}-1 = 268,435,455 = 3 \cdot 5 \cdot 29 \cdot 43 \cdot 113 \cdot 127 & \checkmark \\m_4 &= 2^{29}-1 = 536,870,911 = 233 \cdot 1,103 \cdot 2,089 & \checkmark \\m_5 &= 2^{31}-1 = 2,147,483,647 \text{ (prime)} & \checkmark\end{aligned}$$

Thus, we can uniquely represent all numbers up to

$$m = \prod m_i \approx 1.4 \times 10^{42} \approx 2^{139.5}$$

by their residues r_i modulo these five m_i .

- E.g., ~~10^{30}~~ = ($r_1 = 20,900,945$; $r_2 = 18,304,504$; $r_3 = 65,829,085$;
 $r_4 = 516,865,185$; $r_5 = 1,234,980,730$)

To add two such numbers in this representation,
Just add their corresponding residues
using machine-native 32-bit integers.
Take the result mod 2^k-1 :

If result is \geq the appropriate 2^k-1 value,
subtract out 2^k-1

Note: No carries are needed between
the different pieces!

What's x such that:

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

$$x \equiv a_i \pmod{m_i}$$
$$m = \prod m_i$$
$$y_i = m_i^{-1} \pmod{m_i}$$
$$m_i = m / m_i$$
$$x = \sum a_i y_i m_i \pmod{m}$$

Using the Chinese Remainder theorem let:

$$m = 3 \times 5 \times 7 = 105$$

$$M_1 = m/3 = 105/3 = 35; \quad 2 \text{ is an inverse of } M_1 = 35 \pmod{3} \text{ (since } 35 \times 2 \equiv 1 \pmod{3})$$

$$M_2 = m/5 = 105/5 = 21; \quad 1 \text{ is an inverse of } M_2 = 21 \pmod{5} \text{ (since } 21 \times 1 \equiv 1 \pmod{5})$$

$$M_3 = m/7 = 15; \quad 1 \text{ is an inverse of } M_3 = 15 \pmod{7} \text{ (since } 15 \times 1 \equiv 1 \pmod{7})$$

$$\text{So } x \equiv 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 233 \equiv 23 \pmod{105}$$

So answer: 23

What is the x value in Z_{15} such that

$$x \equiv 1 \pmod{3}$$

$$x \equiv 4 \pmod{5}$$

$$a_1 = 1, m_1 = 3 \quad m = 3 \times 5 = 15$$

$$a_2 = 4, m_2 = 5 \quad M_1 = 5 \\ m_2 = 3$$

$$y_1 = m_1^{-1} \pmod{3} = ?$$

$$y_2 = M_2^{-1} \pmod{5} = ?$$

$$x = a_1 y_1 m_1 + a_2 y_2 m_2 \pmod{15} \\ = 34 \pmod{5} \\ = 4$$

$$x \equiv 6 \pmod{11}$$

$$x \equiv 13 \pmod{16}$$

$$x \equiv 9 \pmod{21}$$

$$x \equiv 19 \pmod{25}$$

Solve ?

$$a_1 = 6 \quad a_2 = 13 \quad a_3 = 9 \quad a_4 = 19$$

$$m_1 = 11 \quad m_2 = 16 \quad m_3 = 21 \quad m_4 = 25$$

$$(m_i, m_j) = 1, \text{ for } i \neq j$$

$$M = \prod m_i = m_1 m_2 m_3 m_4$$

$$= 11 \times 16 \times 21 \times 25$$

$$M_1 = m/m_1 = 16 \times 21 \times 25 = 8400$$

$$M_2 = m/m_2 = 11 \times 21 \times 25 = 5775$$

$$M_3 = m/m_3 = 11 \times 16 \times 25 = 4400$$

$$M_4 = m/m_4 = 11 \times 16 \times 21 = 3696$$

$$x = 2029869 \pmod{92400}$$
$$= 51669 ??$$

$$y_1 = M_1^{-1} \pmod{m_1} = 8$$

$$y_2 = M_2^{-1} \pmod{m_2} = 15$$

$$y_3 = M_3^{-1} \pmod{m_3} = 2$$

$$y_4 = M_4^{-1} \pmod{m_4} = 6$$

Ex: Find all solutions of $x^2 \equiv 1 \pmod{144}$

Sol: $144 = 2^4 \cdot 3^2$ and $\gcd(2^4, 3^2) = 1$

$$m_1 = 16, m_2 = 9$$

$$x^2 \equiv 1 \pmod{16}$$
$$x^2 \equiv 1 \pmod{9}$$

Home work ??

Quadratic Residues

COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF INFORMATION TECHNOLOGY
SRI CITY, INDIA

Groups

$$2 \times_5 4 = 8 \bmod 5 \equiv 3$$

1) Closure: $a+b \in \mathbb{Z}_n$
2) Associative
3) Existence of identity
4) Existence of inverse.

$$(a \times_n b) \times_n c = a \times_n (b +_n c)$$

Additive Group: $+_n$

- $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ forms a group under addition modulo n.

Multiplicative Group:

- $\mathbb{Z}_n^* = \{x \mid 1 \leq x < n \text{ and } \gcd(x, n) = 1\}$ forms a group under multiplication modulo n. \times_n
 - For prime p, \mathbb{Z}_p^* includes all elements $[1, p-1]$.
 - E.g., $\mathbb{Z}_6^* = \{1, 5\}$ ✓
 - E.g., $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ ✓
- $$2 \times_5 4 = 8 \bmod 5 \\ = 3$$

Order and Generator

Order of x : smallest t such that $x^t \equiv 1 \pmod{n}$

- E.g., in Z_{11}^* , $\text{ord}(3) = 5$, $\text{ord}(2) = 10$

Generator: an element whose order = group size.

- E.g., 3 is the generator of Z_7^*

$$3^1 \equiv 3$$

Subgroup: generated from an element of order $t < \Phi(n)$

- $\{1, 3, 3^2=9, 3^3=5, 3^4=4\} = \{1, 3, 4, 5, 9\}$ is a subgroup of Z_{11}^*

$$3^4 \times 3 \equiv 1 \pmod{11}$$

$$(3^5)^2 \equiv 1 \pmod{11}$$

$$(3^5)^3 \equiv 1 \pmod{11}$$

A group is cyclic if it has a generator.

$$3^4 \times 3^4 \equiv 1 \pmod{11}$$

For any prime p , the group Z_p^* is cyclic, i.e, every Z_p^* has a generator, say g .

- $Z_p^* = \{1, g, g^2, g^3, \dots, g^{p-2}\}$

$$\begin{matrix} g & \times \\ 2 & \times \\ \hline g \cdot 2 & \end{matrix}$$

$$\begin{matrix} g & + \\ 2 & \times \\ \hline g+2 & \end{matrix}$$

$$\begin{matrix} g & \times \\ 2 & \times \\ \hline g \cdot 2 & \end{matrix}$$

$$\begin{matrix} g & \times \\ 2 & \times \\ \hline g \cdot 2 & \end{matrix}$$

$$\begin{matrix} g & \times \\ 2 & \times \\ \hline g \cdot 2 & \end{matrix}$$

$$\begin{matrix} g & \times \\ 2 & \times \\ \hline g \cdot 2 & \end{matrix}$$

$$\begin{matrix} g & \times \\ 2 & \times \\ \hline g \cdot 2 & \end{matrix}$$

Quadratic Residue

$$\begin{aligned}x^2 + 1 &= 0 \quad \text{has no solution in } \mathbb{R} \\x^2 &= -1 \quad \text{in } \mathbb{C} \\x &= \pm \sqrt{-1} \\&= \pm i\end{aligned}$$

- y is a **quadratic residue** $(\bmod n)$ if there exists x in \mathbb{Z}_n^* such that $x^2 = y (\bmod n)$
i.e., y has a square root in \mathbb{Z}_n^*
- **Claim:** For any prime p , every quadratic residue has exactly two square roots $x, -x \bmod p$.
- **Proof:** if $x^2 = u^2 \bmod p$, then $(x-u)(x+u) = 0 \bmod p$,
so, either p divides $x-u$ (i.e., $x=u$), or p divides $x+u$ (i.e., $x=-u$)
It implies if $x^2 = 1 \bmod p$, $x = 1$ or -1 .

Quadratic Residue

Theorem: For any prime p , and g is generator,

g^k is a quadratic residue iff k is even.

Given $Z_p^* = \{1, g, g^2, g^3, \dots, g^{p-2}\}$

- Even powers of g are quadratic residues
- Odd powers of g are not quadratic residues

Legendre symbol:

- $\left(\frac{a}{p}\right) = 1$ if a is a quadratic residue mod p ,
- -1 if a is not a quadratic residue mod p ,
- 0 if p divides a .

Euler's Criteria

Theorem: For prime $p > 2$ and a in \mathbb{Z}_p^* , $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}$

- \mathbb{Z}_p^* is cyclic, $a = g^k$ for some k .
- If k is even, let $k = 2m$, $a^{(p-1)/2} = g^{(p-1)m} = 1$.
- If k is odd, let $k = 2m+1$, $a^{(p-1)/2} = g^{(p-1)/2} = -1$.
- Reasons:
 - This is a square root of 1.
 - $g^{(p-1)/2} = 1$ since $\text{ord}(g) = (p-1)/2$.
 - But 1 has two square roots. Thus, the only solution is -1.

If n is prime, $a^{(n-1)/2} = 1$ or -1.

If we find $a^{(n-1)/2}$ is not 1 and -1, n is composite.

$$x^2 = 1 \Rightarrow x = \pm 1$$

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}$$

$$(g^{(p-1)/2})^2 \equiv 1 \pmod{p}$$
$$a = g^k$$
$$\Rightarrow a^2 \equiv 1 \pmod{p}$$

$$\left(\frac{3}{5}\right) = 3^{(5-1)/2} \pmod{5} = -1 \text{ QNR}$$

QNR

$$3^2 \pmod{5} = 4 \pmod{5}$$

$$\begin{aligned} \left(\frac{4}{5}\right) &= ? \\ &\stackrel{(5-1)/2}{=} 4 \pmod{5} \\ &= 4^2 \pmod{5} \\ &= 16 \pmod{5} \\ &= 1 \\ \therefore 4 &\text{ is QR mod } 5 \end{aligned}$$

$$\exists \text{ no } y \in \mathbb{Z}_5^*$$

$$y^2 \equiv 3$$

$$\{3\} \not\in \mathbb{Z}_5^*$$

$$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$$

$$\begin{cases} 1^2 \equiv 1 \pmod{5} \\ 2^2 \equiv 4 \pmod{5} \\ 3^2 \equiv 9 \pmod{5} = 4 \\ 4^2 \equiv 16 \pmod{5} = 1 \end{cases}$$

$$\mathbb{Q}_5 = \{1, 4\}$$

Cippolla's Algorithm

- Let y is a quadratic residue modulo p
- Choose t such that $u = t^2 - y$ is quadratic non-residue
- Then $x = (t + w)^{(p+1)/2}$ gives a square root of y , where $w = \sqrt{u}$
that is, $x^2 = y \text{ mod } p$, if y is quadratic residue.

Quadratic Residue: $\exists y$ such that $x^2 = y \text{ mod } p$

Example: find $\sqrt{2} \text{ mod } 17$

Sol: Is 2 quadratic residue mod 17 ? \rightarrow yes $2 \in QR \text{ mod } 17$.

$$\left(\frac{2}{17}\right) \stackrel{?}{=} 1 \Rightarrow 2^{\frac{(17-1)/2}{2}} \text{ mod } 17 \\ = 2^8 \text{ mod } 17 = 1$$

Let y is a quadratic residue modulo p

Choose t such that $u = t^2 - y$ is quadratic non-residue

Then $x = (t + w)^{(p+1)/2}$ gives a square root of y , where $w = \sqrt{u}$
that is, $x^2 = y \text{ mod } p$, if y is quadratic residue.

Example: find $\sqrt{2} \text{ mod } 17$

$$t=0, \quad u = t^2 - y = 0^2 - 2 \pmod{17} = 15$$
$$15^{\frac{(17-1)/2}{}} = \underline{1} \pmod{17} \quad \text{QR} \quad \times$$

$$t=3, \quad u = 3^2 - 2 = 7 \pmod{17}$$

$$7^8 \pmod{17} = \underline{-1} \quad \text{QNR}$$

$$w = \sqrt{7}, \quad x = (3 + \sqrt{7})^{\frac{(17+1)/2}{}} = (3 + \sqrt{7})^9 \pmod{17}$$

$$(3 + \sqrt{7})^9 = (3 + \sqrt{7})^2 (3 + \sqrt{7})^7$$

$$= 16 + 6\sqrt{7}$$

$$(3 + \sqrt{7})^4 = (3 + \sqrt{7})^2 \times (3 + \sqrt{7})^2$$

$$= (16 + 6\sqrt{7})(16 + 6\sqrt{7})$$

$$= 15 + 5\sqrt{7}$$

Check

$$6^2 \equiv 2 \pmod{17}$$

$$\sqrt{2} = \begin{cases} 6 \pmod{17} \\ 11 \pmod{17} \end{cases}$$

$$(3 + \sqrt{7})^8$$

$$= (3 + \sqrt{7})^4 (3 + \sqrt{7})^4$$

$$= (15 + 5\sqrt{7})(15 + 5\sqrt{7})$$

$$= 9 + 14\sqrt{7}$$

$$(3 + \sqrt{7})^9 = (3 + \sqrt{7})^8 (3 + \sqrt{7})$$

$$= (9 + 14\sqrt{7})(3 + \sqrt{7})$$

$$= 6 \pmod{17}$$

Q: find $\sqrt{2} \pmod{23}$? Q: find $\sqrt{3} \pmod{23}$?

Home work.

Q: There exists an integer x , such that

$$3x \equiv 347 \pmod{453}.$$

Sol:

$ax \equiv b \pmod{m}$ has a solution

$$\text{iff } (a, m) \mid b$$

$$a = 3, b = 347, m = 453$$

$$(a, m) = 3$$

$$3 \nmid 347$$

\therefore No such x exists.

Q: Find the remainder of $\frac{2012}{7}$ upon division by 2011.

Sol: 2011 is prime.

Fermat's Theorem, $\frac{2010}{7} \mod 2011 = 1$

$$\frac{2012}{7} = \frac{\frac{2010}{7} * \frac{2}{7}}{= \quad =} \mod 2011 = 49$$

Q: Find last two decimal digits of 413^{402} .

Hint: The last two decimal digits of a positive integer n are given by the least non-negative residue of $n \mod 100$.

Sol: $413 \equiv 13 \pmod{100}$

$$13^{402} \pmod{\underline{100}}$$

$$13^{\phi(100)} \equiv 1 \pmod{100}$$

$$100 = 2^2 \times 5^2$$

$$\phi(100) = 2^1(2-1) \times 5^1(5-1) \\ = 40$$

$$402 = 40 \times 10 + 2$$

$$13^{402} = (13^{40})^{10} \times 13^2 \pmod{100}$$

$$= 69$$

Q: Find all integer solutions (x, y) of the equation $13x + 11y = 7$.

Hint: first find solution for $13x + 11y = 1$.
Then generalize.

Sol: By Euclidean algorithm, we will get $x = -5, y = 6$.

Let $(x_0, y_0) = (-5, 6)$ for $13x + 11y = 1$.

$(x_1, y_1) = 7(x_0, y_0) = (-35, 42)$ is solution for $13x + 11y = 7$.

$(x, y) = (-35 + 11k, 42 - 13k), k \in \mathbb{Z}$.

Q: prove that, for all integers $n \geq 2$, the number $n^{40}+1$ is composite.
and find a non-trivial divisor of this number.

Hint: try modulo n^8+1 , $40 = 8 \times 5$

$$n^8 \equiv -1 \pmod{n^8+1}$$

$$(n^8)^5 \equiv (-1)^5 \pmod{n^8+1}$$

$$n^{40} \equiv -1 \pmod{n^8+1}$$

$$\underline{n^{40}+1 \equiv 0 \pmod{n^8+1}}$$

Q: prove that, for any integer n , the number $n^3 - n$ is divisible by 35.

fill ??

$$a^{p-1} \equiv 1 \pmod{p},$$

$p \nmid a$

$$35 = 7 \times 5$$

$$p=5, \quad 5 \nmid n \}$$

$5 \mid n$

$$p=7, \quad 7 \nmid n \}$$

$7 \mid n$

TEST(n) is:

1. Find biggest k , $k > 0$, so that $(n-1) = 2^k q$
2. Select a random integer a , $1 < a < n-1$
3. if $a^q \bmod n = 1$ then return ("maybe prime");
4. for $j=0$ to $k-1$ do
 5. if $(a^{2^j q} \bmod n = n-1)$
 then return(" maybe prime ")
6. return ("composite")

$$\left. \begin{array}{l} a^q \bmod n = 1 \times \\ a^q \bmod n = n-1 \times \\ a^{2q} \bmod n = n-1 \times \\ a^{4q} \bmod n = n-1 \\ a^{8q} \bmod n = n-1 \\ a^{16q} \bmod n = n-1 \\ a^{32q} \bmod n = n-1 \end{array} \right\}$$

Q: check 1729 is prime using Miller-Rabin test?

Sol: $1729 - 1 = 1728 = 2^6 \times 27$

$$k = 6, q = 27$$

$$j = 0, 1, 2, 3, 4, 5$$

$$a = 671$$

$$a^q \bmod n = 671 \bmod 1729 = 1084$$

$$a^{2q} \bmod n = (1084)^2 \bmod 1729 = 1065$$

$$a^{4q} \bmod n = (1065)^2 \bmod 1729 = 1$$

Composite.

Q: $n = 104513$ } what is Miller-Rabin Test decision?
 $a = 3$ }

$$n-1 = 104512 = 2^6 \times 1633, j=0, 1, 2, 3, 4, 5$$

$$a^2 = 3^{1633} \pmod{n} = 88958 \not\equiv 1 \pmod{n-1}$$

$$a^{2^2} = (88958)^2 \pmod{n} = 10430 \not\equiv n-1$$

$$a^{2^3} = (10430)^2 \pmod{n} = 91380 \not\equiv n-1$$

$$a^{2^4} = (91380)^2 \pmod{n} = 29239 \not\equiv n-1$$

$$a^{2^5} = (29239)^2 \pmod{n} = 2781 \not\equiv n-1$$

$$a^{2^6} = (2781)^2 \pmod{n} = 104512 = n-1 \checkmark$$

→ n is prime.

$$\underline{Q}: n = 280001, \quad a = 105532$$

check the decision of Miller-Rabin Test?

$$\underline{\text{sol}}: n-1 = 280000 = 2^6 \times 4375$$

$$a^q \equiv (105532)^{4375} \pmod{n} = 236926 \not\equiv 1 \not\equiv n-1$$

$$a^{2^1} = (236926)^2 \pmod{n} = 168999 \not\equiv n-1$$

$$a^{2^2} = (168999)^2 \pmod{n} = 280600 = n-1$$

Conclusion: may be prime.

Shannon's Theory

Dr. Odelu Vanga

Computer Science and Engineering
Indian Institute of Information Technology Sri City

odelu.vanga@iiits.in

January 28, 2021

Today's Objectives

- Discrete Random Variable
- Probability Distribution
- Joint Probability
- Conditional Probability
- Bayes' Theorem

Introduction

- In 1949, Claude Shannon published a paper entitled “**Communication Theory of Secrecy Systems**” in the Bell Systems Technical Journal.
- This paper had a great influence on the scientific study of cryptography.

Computational security

- A cryptosystem is computationally secure if the best algorithm for breaking it requires at least N operations, where N is some specified, very large number.
- The problem is that no known practical cryptosystem can be proved to be secure under this definition.
- In practice, often we study the computational security of a cryptosystem w.r.t. certain specific type of attack. For example, exhaustive key search

Provable security

- Provide evidence of computational security by reducing the security of the cryptosystem to some well-studied problem that is thought to be difficult.
- For example, “**a given cryptosystem is secure if a given integer n cannot be factored**”
- This approach only provides a proof of security relative to some other problem, not an absolute proof of security.

Unconditional security

A cryptosystem is defined to be unconditionally secure if it cannot be broken, even with infinite computational resources

Discrete Random Variable

- An **experiment** is a procedure that yields one a given set of outcomes.
- Individual outcomes are called **sample events**
- The set of all possible outcomes called **sample space**, denoted by S .

Definition (Random Variable (r.v.))

A r.v. is a function, say X , is a function from the sample space S to the set of real numbers.

A r.v X takes finite or countably infinite number of values called a **discrete r.v.**

Probability Distribution

Definition (Discrete Probability Distribution)

Let X be a discrete r.v., and suppose that the possible values that it can take are x . The probability that the random variable X takes value x is denoted by $\Pr[X = x]$, and must satisfy the following

$$\Pr[X = x] \geq 0, \text{ for all } x \in X$$

$$\sum_{x \in X} \Pr[X = x] = 1$$

Example: Tossing pair of fair coins

Joint and Conditional Probability

- probability that X takes on the value x by $Pr[x]$
- probability that Y takes on the value y by $Pr[y]$

Definition (Joint Probability)

Suppose X and Y are random variables. The joint probability $Pr[x, y]$ is the probability that X takes on the value x and Y takes on value y .

Definition (Conditional Probability)

The conditional probability $Pr[x|y]$ denotes the probability that X takes on the value x given that Y takes on the value y .

Example: Tossing pair of fair dice

Bayes' Theorem

Joint probability can be related to conditional probability by the formula

$$Pr[x, y] = Pr[x|y]Pr[y]$$

Then we have

$$Pr[x, y] = Pr[y|x]Pr[x]$$

Theorem (Bayes' Theorem)

If $Pr[y] > 0$, then

$$Pr[x|y] = \frac{Pr[x]Pr[y|x]}{Pr[y]}$$

The random variables X and Y are said to be independent if $Pr[x, y] = Pr[x]Pr[y]$ for all possible values x of X and y of Y .

Perfect Secrecy

Assumptions:

1. Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is specified.
2. A particular key $k \in \mathcal{K}$ is used for only one encryption.
3. Plaintext \mathcal{P} defines a r.v. denoted by X , and a prior probability that plaintext occurs denoted by $Pr[X = x]$.
4. The key chosen with some fixed probability distribution, so key also defines a r.v., denoted by K . Denote the probability that key K is chosen by $pr[K = k]$.
5. The probability distributions on \mathcal{P} and \mathcal{K} induce a probability distribution on \mathcal{C} . So, ciphertext also a r.v., denoted by Y .

Note that key is chosen before the plaintext knows, so that plaintext and key are independent r.v.'s.

Perfect Secrecy

- For a key $k \in \mathcal{K}$, we define

$$\mathcal{C}(k) = \{E_k(x) : x \in \mathcal{P}\}$$

The set of all possible ciphertexts if k is the key

- For every $y \in \mathcal{C}$, we have

$$Pr[Y = y] = \sum_{\{k:y \in \mathcal{C}(k)\}} Pr[K = k] Pr[X = D_k(y)]$$

Note $x = D_k(E_k(x)) = D_k(y)$

- For $y \in \mathcal{C}$ and $x \in \mathcal{P}$, we have

$$Pr[Y = y | X = x] = \sum_{\{k:x=D_k(y)\}} Pr[K = k]$$

Bayes' Theorem

$$Pr[X = x | Y = y] = \frac{Pr[X = x] \sum_{\{k : x = D_k(y)\}} Pr[K = k]}{\sum_{\{k : y \in C(k)\}} Pr[K = k] Pr[X = D_k(y)]}$$

Example

Let $\mathcal{P} = \{a, b\}$ with $Pr[a] = 1/4$, $Pr[b] = 3/4$

$\mathcal{K} = \{k_1, k_2, k_3\}$ with $Pr[k_1] = 1/2$, $Pr[k_2] = Pr[k_3] = 1/4$,
and $\mathcal{C} = \{1, 2, 3, 4\}$.

Suppose encryption rule is defined as

$E_k(x)$	a	b
k_1	1	2
k_2	2	3
k_3	3	4

Find the probability $Pr[X = x | Y = y]$

Shannon's Theory

Dr. Odelu Vanga

Computer Science and Engineering
Indian Institute of Information Technology Sri City

odelu.vanga@iiits.in

Feb. 02, 2021

Perfect Secrecy

Assumptions:

1. Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is specified.

Perfect Secrecy

Assumptions:

1. Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is specified.
2. A particular key $k \in \mathcal{K}$ is used for only one encryption.

Perfect Secrecy

Assumptions:

1. Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is specified.
2. A particular key $k \in \mathcal{K}$ is used for only one encryption.
3. Plaintext \mathcal{P} defines a r.v. denoted by X , and a prior probability that plaintext occurs denoted by $Pr[X = x]$.

Perfect Secrecy

Assumptions:

1. Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is specified.
2. A particular key $k \in \mathcal{K}$ is used for only one encryption.
3. Plaintext \mathcal{P} defines a r.v. denoted by X , and a prior probability that plaintext occurs denoted by $Pr[X = x]$.
4. The key chosen with some fixed probability distribution, so key also defines a r.v., denoted by K . Denote the probability that key K is chosen by $pr[K = k]$.

Perfect Secrecy

Assumptions:

1. Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is specified.
2. A particular key $k \in \mathcal{K}$ is used for only one encryption.
3. Plaintext \mathcal{P} defines a r.v. denoted by X , and a prior probability that plaintext occurs denoted by $Pr[X = x]$.
4. The key chosen with some fixed probability distribution, so key also defines a r.v., denoted by K . Denote the probability that key K is chosen by $pr[K = k]$.
5. The probability distributions on \mathcal{P} and \mathcal{K} induce a probability distribution on \mathcal{C} . So, ciphertext also a r.v., denoted by Y .

Perfect Secrecy

Assumptions:

1. Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is specified.
2. A particular key $k \in \mathcal{K}$ is used for only one encryption.
3. Plaintext \mathcal{P} defines a r.v. denoted by X , and a prior probability that plaintext occurs denoted by $Pr[X = x]$.
4. The key chosen with some fixed probability distribution, so key also defines a r.v., denoted by K . Denote the probability that key K is chosen by $pr[K = k]$.
5. The probability distributions on \mathcal{P} and \mathcal{K} induce a probability distribution on \mathcal{C} . So, ciphertext also a r.v., denoted by Y .

Note that key is chosen before the plaintext knows, so that plaintext and key are independent r.v.'s.

Perfect Secrecy

- For a key $k \in \mathcal{K}$, we define

$$C(k) = \{E_k(x) : x \in \mathcal{P}\}$$

The set of all possible ciphertexts if k is the key

Perfect Secrecy

- For a key $k \in \mathcal{K}$, we define

$$\mathcal{C}(k) = \{E_k(x) : x \in \mathcal{P}\}$$

The set of all possible ciphertexts if k is the key

- For every $y \in \mathcal{C}$, we have

$$Pr[Y = y] = \sum_{\{k : y \in \mathcal{C}(k)\}} Pr[K = k] Pr[X = D_k(y)]$$

Note $x = D_k(E_k(x)) = D_k(y)$

Perfect Secrecy

- For a key $k \in \mathcal{K}$, we define

$$\mathcal{C}(k) = \{E_k(x) : x \in \mathcal{P}\}$$

The set of all possible ciphertexts if k is the key

- For every $y \in \mathcal{C}$, we have

$$Pr[Y = y] = \sum_{\{k:y \in \mathcal{C}(k)\}} Pr[K = k] Pr[X = D_k(y)]$$

Note $x = D_k(E_k(x)) = D_k(y)$

- For $y \in \mathcal{C}$ and $x \in \mathcal{P}$, we have

$$Pr[Y = y | X = x] = \sum_{\{k:x=D_k(y)\}} Pr[K = k]$$

Bayes' Theorem

$$Pr[X = x | Y = y] = \frac{Pr[X = x] \sum_{\{k: x = D_k(y)\}} Pr[K = k]}{\sum_{\{k: y \in C(k)\}} Pr[K = k] Pr[X = D_k(y)]}$$

Bayes' Theorem

$$Pr[X = x | Y = y] = \frac{Pr[X = x] \sum_{\{k : x = D_k(y)\}} Pr[K = k]}{\sum_{\{k : y \in C(k)\}} Pr[K = k] Pr[X = D_k(y)]}$$

Example

Let $\mathcal{P} = \{a, b\}$ with $Pr[a] = 1/4$, $Pr[b] = 3/4$

$\mathcal{K} = \{k_1, k_2, k_3\}$ with $Pr[k_1] = 1/2$, $Pr[k_2] = Pr[k_3] = 1/4$,
and $\mathcal{C} = \{1, 2, 3, 4\}$.

Suppose encryption rule is defined as

$E_k(x)$	a	b
k_1	1	2
k_2	2	3
k_3	3	4

Find the probability $Pr[X = x | Y = y]$

Perfect Secrecy

Definition

A cryptosystem has perfect secrecy if

$$\Pr[X = x | Y = y] = \Pr[X = x]$$

for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.

Perfect Secrecy

Definition

A cryptosystem has perfect secrecy if

$$\Pr[X = x | Y = y] = \Pr[X = x]$$

for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.

Theorem

Suppose the 26 keys in the Shift Cipher are used with equal probability 1/26. Then for any plaintext probability distribution, the Shift Cipher has perfect secrecy

Perfect Secrecy

Definition

A cryptosystem has perfect secrecy if

$$\Pr[X = x | Y = y] = \Pr[X = x]$$

for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.

Theorem

Suppose the 26 keys in the Shift Cipher are used with equal probability 1/26. Then for any plaintext probability distribution, the Shift Cipher has perfect secrecy

We have, $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$, and define encryption rule as

$$y = E_k(x) = (x + k) \pmod{26}$$

where $x \in \mathcal{P}$ and $k \in \mathcal{K}$.

Theorem

Suppose $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is a cryptosystem, where $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$.

Then

the cryptosystem provides perfect secrecy

if and only if

Theorem

Suppose $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is a cryptosystem, where $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$.

Then

the cryptosystem provides perfect secrecy

if and only if

- every key is used with equal probability $1/|\mathcal{K}|$, and

Theorem

Suppose $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is a cryptosystem, where $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$.

Then

the cryptosystem provides perfect secrecy

if and only if

- every key is used with equal probability $1/|\mathcal{K}|$, and
- for every $x \in \mathcal{P}$ and for every $y \in \mathcal{C}$, there is a unique key k such that $E_k(x) = y$

Perfect Secrecy

Proof.

Suppose the given cryptosystem provides perfect secrecy

Perfect Secrecy

Proof.

Suppose the given cryptosystem provides perfect secrecy

For each $x \in \mathcal{P}$ and $y \in \mathcal{C}$,

there must be at least one key k such that $E_k(x) = y$.

Perfect Secrecy

Proof.

Suppose the given cryptosystem provides perfect secrecy

For each $x \in \mathcal{P}$ and $y \in \mathcal{C}$,

there must be at least one key k such that $E_k(x) = y$.

So, we have the inequalities

$$|\mathcal{C}| = |\{E_k(x) : k \in \mathcal{K}\}| \leq |\mathcal{K}|$$

Perfect Secrecy

Proof.

Suppose the given cryptosystem provides perfect secrecy

For each $x \in \mathcal{P}$ and $y \in \mathcal{C}$,

there must be at least one key k such that $E_k(x) = y$.

So, we have the inequalities

$$|\mathcal{C}| = |\{E_k(x) : k \in \mathcal{K}\}| \leq |\mathcal{K}|$$

But, we assume that $|\mathcal{C}| = |\mathcal{K}|$.

Perfect Secrecy

Proof.

Suppose the given cryptosystem provides perfect secrecy

For each $x \in \mathcal{P}$ and $y \in \mathcal{C}$,

there must be at least one key k such that $E_k(x) = y$.

So, we have the inequalities

$$|\mathcal{C}| = |\{E_k(x) : k \in \mathcal{K}\}| \leq |\mathcal{K}|$$

But, we assume that $|\mathcal{C}| = |\mathcal{K}|$.

Hence, it must be the case that

$$|\{E_k(x) : k \in \mathcal{K}\}| = |\mathcal{K}|$$

Perfect Secrecy

Proof.

Suppose the given cryptosystem provides perfect secrecy

For each $x \in \mathcal{P}$ and $y \in \mathcal{C}$,

there must be at least one key k such that $E_k(x) = y$.

So, we have the inequalities

$$|\mathcal{C}| = |\{E_k(x) : k \in \mathcal{K}\}| \leq |\mathcal{K}|$$

But, we assume that $|\mathcal{C}| = |\mathcal{K}|$.

Hence, it must be the case that

$$|\{E_k(x) : k \in \mathcal{K}\}| = |\mathcal{K}|$$

That is, there do not exist two distinct keys k_1 and k_2 such that $E_{k_1}(x) = E_{k_2}(x) = y$.

Perfect Secrecy

Proof.

Suppose the given cryptosystem provides perfect secrecy

For each $x \in \mathcal{P}$ and $y \in \mathcal{C}$,

there must be at least one key k such that $E_k(x) = y$.

So, we have the inequalities

$$|\mathcal{C}| = |\{E_k(x) : k \in \mathcal{K}\}| \leq |\mathcal{K}|$$

But, we assume that $|\mathcal{C}| = |\mathcal{K}|$.

Hence, it must be the case that

$$|\{E_k(x) : k \in \mathcal{K}\}| = |\mathcal{K}|$$

That is, there do not exist two distinct keys k_1 and k_2 such that

$$E_{k_1}(x) = E_{k_2}(x) = y.$$

Hence, we have shown that for any $x \in \mathcal{P}$ and $y \in \mathcal{C}$, there is exactly one key k such that $E_k(x) = y$.



Perfect Secrecy

Continue.....

Denote $n = |\mathcal{K}|$.

Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$.

Perfect Secrecy

Continue.....

Denote $n = |\mathcal{K}|$.

Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$.

Suppose the keys are k_1, k_2, \dots, k_n , such that $E_{k_i}(x_i) = y, 1 \leq i \leq n$.

Perfect Secrecy

Continue.....

Denote $n = |\mathcal{K}|$.

Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$.

Suppose the keys are k_1, k_2, \dots, k_n , such that $E_{k_i}(x_i) = y, 1 \leq i \leq n$.

Using Bayes' theorem, we have

$$Pr[x_i|y] = \frac{Pr[y|x_i]Pr[x_i]}{Pr[y]} = \frac{Pr[k_i]Pr[x_i]}{Pr[y]}$$

Perfect Secrecy

Continue.....

Denote $n = |\mathcal{K}|$.

Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$.

Suppose the keys are k_1, k_2, \dots, k_n , such that $E_{k_i}(x_i) = y, 1 \leq i \leq n$.

Using Bayes' theorem, we have

$$Pr[x_i|y] = \frac{Pr[y|x_i]Pr[x_i]}{Pr[y]} = \frac{Pr[k_i]Pr[x_i]}{Pr[y]}$$

- Consider the perfect secrecy condition $Pr[x_i|y] = Pr[x_i]$.

Perfect Secrecy

Continue.....

Denote $n = |\mathcal{K}|$.

Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$.

Suppose the keys are k_1, k_2, \dots, k_n , such that $E_{k_i}(x_i) = y$, $1 \leq i \leq n$.

Using Bayes' theorem, we have

$$Pr[x_i|y] = \frac{Pr[y|x_i]Pr[x_i]}{Pr[y]} = \frac{Pr[k_i]Pr[x_i]}{Pr[y]}$$

- Consider the perfect secrecy condition $Pr[x_i|y] = Pr[x_i]$.
- This implies that, $Pr[k_i] = Pr[y]$, for $1 \leq i \leq n$.

Perfect Secrecy

Continue.....

Denote $n = |\mathcal{K}|$.

Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$.

Suppose the keys are k_1, k_2, \dots, k_n , such that $E_{k_i}(x_i) = y$, $1 \leq i \leq n$.

Using Bayes' theorem, we have

$$Pr[x_i|y] = \frac{Pr[y|x_i]Pr[x_i]}{Pr[y]} = \frac{Pr[k_i]Pr[x_i]}{Pr[y]}$$

- Consider the perfect secrecy condition $Pr[x_i|y] = Pr[x_i]$.
- This implies that, $Pr[k_i] = Pr[y]$, for $1 \leq i \leq n$.
- This says that all keys are used with equal probability (namely, $Pr[y]$).

Perfect Secrecy

Continue.....

Denote $n = |\mathcal{K}|$.

Let $\mathcal{P} = \{x_i : 1 \leq i \leq n\}$ and fix a ciphertext element $y \in \mathcal{C}$.

Suppose the keys are k_1, k_2, \dots, k_n , such that $E_{k_i}(x_i) = y$, $1 \leq i \leq n$.

Using Bayes' theorem, we have

$$Pr[x_i|y] = \frac{Pr[y|x_i]Pr[x_i]}{Pr[y]} = \frac{Pr[k_i]Pr[x_i]}{Pr[y]}$$

- Consider the perfect secrecy condition $Pr[x_i|y] = Pr[x_i]$.
- This implies that, $Pr[k_i] = Pr[y]$, for $1 \leq i \leq n$.
- This says that all keys are used with equal probability (namely, $Pr[y]$).
- Since the number of keys are $|\mathcal{K}|$, we must have that $Pr[k] = 1/|\mathcal{K}|$, for $k \in \mathcal{K}$.

Perfect Secrecy

Could you prove the converse of the theorem ?

Continue.....

Given

- every key is used with equal probability $1/|\mathcal{K}|$, and
- for every $x \in \mathcal{P}$ and for every $y \in \mathcal{C}$, there is a unique key k such that $E_k(x) = y$

Prove the cryptosystem provides perfect secrecy.



Bayes' theorem:

$$Pr[X = x | Y = y] = \frac{Pr[X = x] \sum_{\{k: x = D_k(y)\}} Pr[K = k]}{\sum_{\{k: y \in C(k)\}} Pr[K = k] Pr[X = D_k(y)]}$$

Latin Square

Let n be a positive integer. A Latin square of order n is an $n \times n$ array L of the integers $1, \dots, n$ such that every one of the n integers occurs exactly once in each row and each column of L .

Latin Square

Let n be a positive integer. A Latin square of order n is an $n \times n$ array L of the integers $1, \dots, n$ such that every one of the n integers occurs exactly once in each row and each column of L .

An example of a Latin square of order 3 is as follows:

1	2	3
3	1	2
2	3	1

Latin Square

Let n be a positive integer. A Latin square of order n is an $n \times n$ array L of the integers $1, \dots, n$ such that every one of the n integers occurs exactly once in each row and each column of L .

An example of a Latin square of order 3 is as follows:

1	2	3
3	1	2
2	3	1

Given any Latin square L of order n , we can define a related cryptosystem. Take $\mathcal{P} = \mathcal{C} = \mathcal{K}$. For $1 \leq i \leq n$, the encryption rule defined as

$$E_i(j) = L(i, j)$$

(Hence each row of L gives rise to one encryption rule.)

Latin Square

Let n be a positive integer. A Latin square of order n is an $n \times n$ array L of the integers $1, \dots, n$ such that every one of the n integers occurs exactly once in each row and each column of L .

An example of a Latin square of order 3 is as follows:

1	2	3
3	1	2
2	3	1

Given any Latin square L of order n , we can define a related cryptosystem. Take $\mathcal{P} = \mathcal{C} = \mathcal{K}$. For $1 \leq i \leq n$, the encryption rule defined as

$$E_i(j) = L(i, j)$$

(Hence each row of L gives rise to one encryption rule.)

Give a complete proof that this Latin square cryptosystem achieves perfect secrecy provided that every key is used with equal probability.

One-Time Pad

- One well-known realization of perfect secrecy is the Vernam One-time Pad.
- First described by Gilbert Vernam in 1917 for use in automatic encryption and decryption of telegraph messages.
- One-time Pad was thought for many years to be an “unbreakable” cryptosystem.
- But, there was no proof of this until Shannon developed the concept of perfect secrecy over 30 years later.

One-Time Pad

Definition (One-Time Pad)

Let $n \geq 1$ be an integer, and take $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$. If $k = (k_1, k_2, \dots, k_n)$ in \mathcal{K} ,
 $x = (x_1, x_2, \dots, x_n)$ in \mathcal{P} , and
 $y = (y_1, y_2, \dots, y_n)$ in \mathcal{C} ,
we define

One-Time Pad

Definition (One-Time Pad)

Let $n \geq 1$ be an integer, and take $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$. If $k = (k_1, k_2, \dots, k_n)$ in \mathcal{K} ,
 $x = (x_1, x_2, \dots, x_n)$ in \mathcal{P} , and
 $y = (y_1, y_2, \dots, y_n)$ in \mathcal{C} ,
we define

$$E_k(x) = (x_1 + k_1, x_2 + k_2, \dots, x_n + k_n) \pmod{2}$$

$$D_k(y) = (y_1 + k_1, y_2 + k_2, \dots, y_n + k_n) \pmod{2}$$

Decryption is also identical to the encryption.

One-Time Pad

Definition (One-Time Pad)

Let $n \geq 1$ be an integer, and take $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$. If $k = (k_1, k_2, \dots, k_n)$ in \mathcal{K} ,
 $x = (x_1, x_2, \dots, x_n)$ in \mathcal{P} , and
 $y = (y_1, y_2, \dots, y_n)$ in \mathcal{C} ,
we define

$$E_k(x) = (x_1 + k_1, x_2 + k_2, \dots, x_n + k_n) \pmod{2}$$

$$D_k(y) = (y_1 + k_1, y_2 + k_2, \dots, y_n + k_n) \pmod{2}$$

Decryption is also identical to the encryption.

Note that $\pmod{2}$ is equivalent to the exclusive-or (\oplus).

One-Time Pad - Drawbacks

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		
plaintext (m)	,	.	:	;	space	,								
Assigned No.	26	27	28	29	30		31							

Assume 5-bit character representation

One-Time Pad - Drawbacks

plaintext (m)	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Assigned No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13
plaintext (m)	o	p	q	r	s	t	u	v	w	x	y	z		
Assigned No.	14	15	16	17	18	19	20	21	22	23	24	25		
plaintext (m)	,	.	:	;	space	,								
Assigned No.	26	27	28	29	30		31							

Assume 5-bit character representation

Example (One key for one encryption)

Generate a ciphertext with random key given by *I am good* for the message *it's true* using the above character encoding.

One-Time Pad - Perfect Secrecy

Definition

A cipher (E, D) over $(\mathcal{K}, \mathcal{P}, \mathcal{C})$ has perfect secrecy if $\forall x_0, x_1 \in \mathcal{P}$, $(|x_0| = |x_1|)$ and $\forall y \in \mathcal{C}$

$$\Pr[E_k(x_0) = y] = \Pr[E_k(x_1) = y]$$

where $k \leftarrow_R \mathcal{K}$.

One-Time Pad - Perfect Secrecy

Definition

A cipher (E, D) over $(\mathcal{K}, \mathcal{P}, \mathcal{C})$ has perfect secrecy if $\forall x_0, x_1 \in \mathcal{P}$, $(|x_0| = |x_1|)$ and $\forall y \in \mathcal{C}$

$$\Pr[E_k(x_0) = y] = \Pr[E_k(x_1) = y]$$

where $k \leftarrow_R \mathcal{K}$.

Theorem

The one-time pad encryption scheme is perfectly secure.

One-Time Pad - Perfect Secrecy

Definition

A cipher (E, D) over $(\mathcal{K}, \mathcal{P}, \mathcal{C})$ has perfect secrecy if $\forall x_0, x_1 \in \mathcal{P}$, $(|x_0| = |x_1|)$ and $\forall y \in \mathcal{C}$

$$\Pr[E_k(x_0) = y] = \Pr[E_k(x_1) = y]$$

where $k \leftarrow_R \mathcal{K}$.

Theorem

The one-time pad encryption scheme is perfectly secure.

Proof(One-time pad : perfect secrecy).

We have to show $\forall x_0, x_1 \in \mathcal{P}$, $(|x_0| = |x_1|)$ and $\forall y \in \mathcal{C}$

$$\Pr[E_k(x_0) = y] = \Pr[E_k(x_1) = y]$$



One-Time Pad - Drawbacks

- Vernam patented his idea in the hope that it would have widespread commercial use.
- The fact that $|\mathcal{K}| \geq |\mathcal{P}|$, means that the amount of key that must be communicated securely is **at least as big as the amount of plaintext**.
- This would not be a major problem **if the same key could be used to encrypt different messages**; however, the security of unconditionally secure cryptosystems depends on the fact that **each key is used for only one encryption**.

One-Time Pad - Drawbacks

- Vernam patented his idea in the hope that it would have widespread commercial use.
- The fact that $|\mathcal{K}| \geq |\mathcal{P}|$, means that the amount of key that must be communicated securely is **at least as big as the amount of plaintext**.
- This would not be a major problem **if the same key could be used to encrypt different messages**; however, the security of unconditionally secure cryptosystems depends on the fact that **each key is used for only one encryption**.
- The One-time Pad is **vulnerable to a known-plaintext attack**

Shannon's Theory

Dr. Odelu Vanga
Computer Science and Engineering
Indian Institute of Information Technology Sri City
odelu.vanga@iiits.in

Entropy (1948) :

→ A mathematical measure of information/uncertainty.

X - (finite) r.v.

Ex: X toss a coin
 $\Pr[H] = \Pr[T] = \frac{1}{2}$
 1 0

Entropy one bit.

| n -independent tosses of a coin
⇒ Entropy ?? n -bit

1 2 3 4 ... n
0/1 0/1 0/1 ... 0/1

4-bit number.

⇒ 0/1 0/1 0/1 0/1
= = = =

Ex:

$$X = x_1, x_2, x_3$$

$$\Pr[X=x] \quad \begin{matrix} 1/2 & 1/4 & 1/4 \end{matrix}$$

$$\left. \begin{array}{l} x_1 \text{ as } 0 \\ x_2 \text{ as } 10 \\ x_3 \text{ as } 11 \end{array} \right\}$$

$$\frac{1}{2} \times 1 + \frac{1}{4} \times 2 + \frac{1}{4} \times 2 = \frac{3}{2}$$

Entropy: Suppose X is a discrete r.v.

$$H(X) = - \sum_{x \in X} \Pr[x] \log_2 \Pr[x]$$

Remark: If $y=0$, $\log_2 y$ is undefined

$$\lim_{y \rightarrow 0^+} y \log_2 y = 0$$

?

→ If $|X|=n$, $\Pr[x] = \gamma_n$ $\forall x \in X$

Then $H(X) = \log_2 n$

① $H(X) \geq 0$ \forall r.v. X

② $H(X) = 0$ iff $\Pr[x_0] = 1$ for $x_0 \in X$

$\Pr[x] = 0$ for $x \neq x_0$.

Ex:

$$P = \{a, b\}$$

$$\mathcal{K} = \{k_1, k_2, k_3\}$$

$$\mathcal{T} = \{1, 2, 3, 4\}$$

$$\Pr[a] = \frac{1}{4}, \Pr[b] = \frac{3}{4}$$

$$\Pr[k_1] = \frac{1}{2}, \Pr[k_2] = \Pr[k_3] = \frac{1}{4}$$

	a	s
k ₁	1	2
k ₂	2	3
k ₃	3	4

Q: $H(P)$?

$H(\mathcal{K})$?

$H(\mathcal{T})$?

Sol:

$$H(x) = - \sum_{x} \text{pr}[x] \log_2 \text{pr}[x]$$

$$\begin{aligned} H(P) &= - \left(\text{pr}[a] \log_2 \text{pr}[a] + \text{pr}[s] \log_2 \text{pr}[s] \right) \\ &= - \left(\frac{1}{4} \log_2 \frac{1}{4} + \frac{3}{4} \log_2 \frac{3}{4} \right) \\ &= 0.81 \end{aligned}$$

$$\begin{aligned} H(k) &= - \left(\text{pr}[k_1] \log_2 \text{pr}[k_1] + \text{pr}[k_2] \log_2 \text{pr}[k_2] + \text{pr}[k_3] \log_2 \text{pr}[k_3] \right) \\ &= - \left(\frac{1}{2} \log_2 \frac{1}{2} + \frac{1}{4} \log_2 \frac{1}{4} + \frac{1}{4} \log_2 \frac{1}{4} \right) \\ &= \frac{3}{2} = 1.5 \end{aligned}$$

$$\begin{aligned}
 H(c) &= - \left(\Pr[1] \log_2 \Pr[1] \right. \\
 &\quad + \Pr[2] \log_2 \Pr[2] \\
 &\quad + \Pr[3] \log_2 \Pr[3] \\
 &\quad \left. + \Pr[4] \log_2 \Pr[4] \right) \\
 &= - \left(\frac{1}{8} \log \frac{1}{8} + \frac{7}{16} \log \frac{7}{16} \right. \\
 &\quad \left. + \frac{1}{4} \log \frac{1}{4} + \frac{3}{16} \log \frac{3}{16} \right) \\
 &= 1.85
 \end{aligned}$$

$$\Pr[Y=y] = \sum_{k : y \in C(k)} \Pr[k] \Pr[X=D_k(y)]$$

$$\begin{aligned}
 \Pr[1] &= \Pr[k_1] \Pr[a] \\
 &= \frac{1}{2} \times \frac{1}{4} = \frac{1}{8} \\
 \Pr[2] &= \Pr[k_1] \Pr[b] \\
 &\quad + \Pr[k_2] \Pr[a] \\
 &= \frac{1}{2} \times \frac{3}{4} + \frac{1}{4} \times \frac{1}{4} \\
 &= \frac{7}{16}
 \end{aligned}$$

Jensen's Inequality:

Suppose f is a continuous strictly concave function on the interval I ,

$$\sum_{i=1}^n q_i = 1 \text{ and } q_i > 0, \quad 1 \leq i \leq n.$$

Then

$$\sum_{i=1}^n q_i f(x_i) \leq f\left(\sum_{i=1}^n q_i x_i\right)$$

where $x_i \in I, \quad 1 \leq i \leq n$

The equality occurs

$$\text{if } x_1 = x_2 = \dots = x_n.$$

Note: $\log x$ is always
strictly concave
on the $(0, \infty)$

Theorem: Suppose X is a r.v. having prob. distribution, which takes on the values p_1, p_2, \dots, p_n , where $p_i > 0$, $1 \leq i \leq n$.

Then $H(X) \leq \log_2 n$, with equality if $p_i = \frac{1}{n}$, $1 \leq i \leq n$.

Proof:

$$H(X) = - \sum_{i=1}^n p_i \log_2 p_i$$

$$= \sum_{i=1}^n p_i \log_2 \frac{1}{p_i}$$

$$\leq \log_2 \left(\sum_{i=1}^n p_i \times \frac{1}{p_i} \right)$$

Jensen's inequality

$$= \log_2 n$$

$$\Rightarrow H(X) \leq \log_2 n.$$

*

	a	b	c	-	\$
k ₁	1	2	3		
k ₂	2	3	4		
k ₃	3	4	1		
S					

$$P = \{a, b, c\}$$

$$S = \{k_1, k_2, k_3\}$$

$$\mathcal{T} = \{1, 2, 3, 4\}$$

Q3). What is H(τ)?

Q1) $Pr[a] = \frac{1}{2}, Pr[b] = \frac{1}{3}, Pr[c] = \frac{1}{6}$

$$H(P) ?$$

Q2) $Pr[k_1] = Pr[k_2] = Pr[k_3] = \frac{1}{3}$

$$H(S) ?$$

Shannon's Theory

Dr. Odelu Vanga
Computer Science and Engineering
Indian Institute of Information Technology Sri City
odelu.vanga@iiits.in

Conditional Entropy :

Suppose X & Y are two r.v.

Then for any fixed $y \in Y$, we get a conditional probability distribution

on X ,

$$H(X|y) = - \sum_x \text{pr}[x|y] \log_2 \text{pr}[x|y].$$

$$\underline{H(X|Y)} = - \sum_y \sum_x \text{pr}[y] \text{pr}[x|y] \log_2 \text{pr}[x|y].$$

Note: Measures the average amount of information about X that is revealed by Y .

EX: Consider cryptosystems

$$\mathcal{P} = \{a, b, c\}$$

$$\mathcal{K} = \{k_1, k_2, k_3\}$$

$$\mathcal{C} = \{1, 2, 3, 4\}$$

$$Q : H(\mathcal{P})$$

$$H(\mathcal{K})$$

$$H(\mathcal{C})$$

Encryption

$E_K(x)$	a	b	c
k_1	1	2	3
k_2	2	3	4
k_3	3	4	1

$$pr[a] = \gamma_2, pr[b] = \gamma_3$$

$$pr[c] = \gamma_6$$

$$pr[k_1] = pr[k_2] = pr[k_3] = \gamma_3.$$

$H(\mathcal{K}|C)$ - Key Escalation

$$\text{Solu: } H(X) = - \sum_{x} \text{pr}[x] \log_2 \text{pr}[x]$$

$$H(P) = - \left(\text{pr}[a] \log_2 \text{pr}[a] + \text{pr}[s] \log_2 \text{pr}[s] + \text{pr}[c] \log_2 \text{pr}[c] \right)$$

$$= - \left(\frac{1}{2} \log_2 \frac{1}{2} + \frac{1}{3} \log_2 \frac{1}{3} + \frac{1}{6} \log_2 \frac{1}{6} \right)$$

$$= \frac{1}{2} \log_2 2 + \frac{1}{3} \log_2 3 + \frac{1}{6} \log_2 6$$

$$= 1.45915$$

$$H(f) = - \left(\text{pr}[k_1] \log_2 \text{pr}[k_1] + \text{pr}[k_2] \log_2 \text{pr}[k_2] + \text{pr}[k_3] \log_2 \text{pr}[k_3] \right)$$

$$= - \left(\frac{1}{3} \log_2 \frac{1}{3} + \frac{1}{3} \log_2 \frac{1}{3} + \frac{1}{3} \log_2 \frac{1}{3} \right)$$

$$= \log 3$$

$$= 1.58496$$

$$H(C) = - \sum_{y \in C} p_r[y] \log p_r[y]$$

we have to find $p_r[1], p_r[2], p_r[3], p_r[4]$

$$p_r[y] = \sum_{k : y \in c(k)} p_r[k] p_r[x = D_k(y)]$$

$$p_r[1] = 5/18$$

$$p_r[2] = 1/3$$

$$p_r[3] = 2/6$$

$$H(C) =$$

$$p_r[1] = \sum_{k : 1 \in c(k)} p_r[k] p_r[x = D_k(1)]$$

$$c(k_1) = \{1, 2, 3\}$$

$$c(k_2) = \{2, 3, 4\}$$

$$c(k_3) = \{3, 4, 1\}$$

$$p_r[1] = p_r[k_1] p_r[x = a]$$

$$+ p_r[k_3] p_r[c]$$

$$= \frac{1}{3} \times \frac{1}{2} + \frac{1}{3} \times \frac{1}{6}$$

$$= \frac{2}{9}$$

$$H(c) = - \left(p_r[1] \log p_r[1] + p_r[2] \log p_r[2] + p_r[3] \log p_r[3] + p_r[4] \log p_r[4] \right)$$

$$= - \left(\frac{2}{9} \log \frac{2}{9} + \frac{5}{18} \log \frac{5}{18} + \frac{1}{3} \log \frac{1}{3} + \frac{1}{6} \log \frac{1}{6} \right)$$

$$= \frac{2}{9} \log \frac{9}{2} + \frac{5}{18} \log \frac{18}{5} + \frac{1}{3} \log 3 + \frac{1}{6} \log 6$$

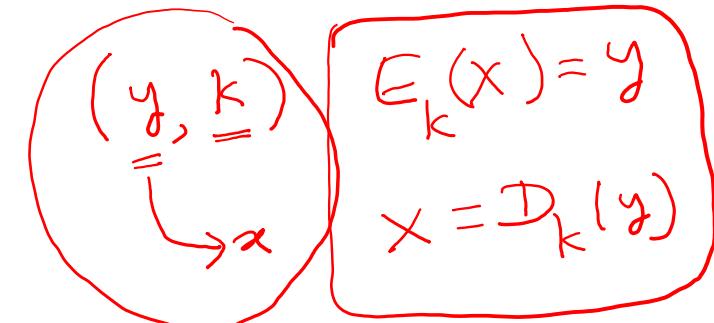
$$= 1.95469$$

$$H(k|c) = - \sum_y \sum_k \Pr[y] \Pr[k|y] \log \Pr[k|y].$$

$$\Pr[k|y] = \frac{\Pr[k] \Pr[y|k]}{\Pr[y]}$$

$$\Pr[k_i|z] = \frac{\Pr[k] \Pr[z|k]}{\Pr[z]}$$

$$\left. \begin{aligned} & \Pr[y=\underline{y} | k=\underline{k}] \\ &= \Pr[E_{\underline{k}}(x)=\underline{y} | k=\underline{k}] \\ &= \Pr[E_{\underline{k}}(x)=\underline{y}] \\ &= \Pr[x=D_{\underline{k}}(\underline{y})] \end{aligned} \right\}$$



State: For given y and K in any cryptosystem,
 \exists only one x with condition $x = D_K(y)$.

Proof: Suppose $\exists x_0 \neq x_1 \ni$

$$y = E_K(x_0), \quad \underline{y = E_K(x_1)}$$

$$x_0 = D_K(E_K(x_0)) = D_K(y) = D_K(E_K(x_1)) = x_1$$

$$\Rightarrow x_0 = x_1$$



Our assumption wrong.

$$\therefore x_0 = x_1$$

Shannon's Theory

Dr. Odelu Vanga
Computer Science and Engineering
Indian Institute of Information Technology Sri City
odelu.vanga@iiits.in

Conditional Entropy :

Suppose X & Y are two r.v.

Then for any fixed $y \in Y$, we get a conditional probability distribution

on X ,

$$H(X|y) = - \sum_x \text{pr}[x|y] \log_2 \text{pr}[x|y].$$

$$\underline{H(X|Y)} = - \sum_y \sum_x \text{pr}[y] \text{pr}[x|y] \log_2 \text{pr}[x|y].$$

Note: Measures the average amount of information about X that is revealed by Y .

EX: Consider cryptosystems

$$\mathcal{P} = \{a, b, c\}$$

$$\mathcal{K} = \{k_1, k_2, k_3\}$$

$$\mathcal{C} = \{1, 2, 3, 4\}$$

$$Q: \begin{array}{l} H(\mathcal{P}) \checkmark \\ H(\mathcal{K}) \checkmark \\ H(\mathcal{C}) \checkmark \end{array}$$

Encryption

$E_K(x)$	a	b	c
k_1	1	2	3
k_2	2	3	4
k_3	3	4	1

$$\Pr[a] = \gamma_2, \Pr[b] = \gamma_3$$

$$\Pr[c] = \gamma_6$$

$$\Pr[k_1] = \Pr[k_2] = \Pr[k_3] = \gamma_3.$$

$H(\mathcal{K}|\mathcal{C})$ - Key Entropy

$$\boxed{\Pr[y=k|x=k] = \Pr[x=D_K(y)]}$$

$$H(\mathcal{X}|\mathcal{C}) = - \sum_y \sum_k \Pr[y] \Pr[k|y] \log \Pr[k|y]$$

$$\Pr[K|y] = \frac{\Pr[K] \Pr[y|K]}{\Pr[y]}$$

$$\Pr[K_1|1] = \frac{\Pr[K_1] \Pr[1|K_1]}{\Pr[1]} = \frac{\frac{1}{3} \cdot \frac{1}{2}}{\frac{2}{9}} = \frac{3}{4}$$

$$\Pr[K_1|2] =$$

$$\Pr[K_1|3] =$$

$$\Pr[K_1|4] =$$

y	1	2	3	4
$\Pr[y]$	$\frac{2}{9}$	$\frac{5}{18}$	$\frac{1}{3}$	$\frac{1}{6}$

$\Pr[K y]$	1	2	3	4
K_1	$\frac{3}{4}$	$\frac{2}{5}$	$\frac{1}{6}$	0
K_2	0	$\frac{3}{5}$	$\frac{1}{3}$	$\frac{1}{3}$
K_3	$\frac{1}{4}$	0	$\frac{1}{2}$	$\frac{2}{3}$

$$H(K|e) = 1.08942$$

$$H(K|e) = - \sum_y \sum_K \Pr[y] \Pr[K|y] \log \Pr[K|y]$$

$$\Rightarrow H(K|e) = H(K) + H(P) - H(e)$$

Ex: $P = \{a, \delta\}$ $Pr[a] = 1/4$, $Pr[\delta] = 3/4$

$\mathcal{F} = \{k_1, k_2, k_3\}$ $Pr[k_1] = 1/2$, $Pr[k_2] = Pr[k_3] = 1/4$

$\tau = \{1, 2, 3, 4\}$

	a	δ
k_1	1	2
k_2	2	3
k_3	3	4

Q). $H(\mathcal{F} | \tau) = ?$

Home work
practice.??