SCIM106
AY24/25 SEM 2
miimi

RSA Encryption Process

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Step 1: RSA Setup
- Public key: $n = 29 \times 31 = 899, \; e = 41$
- Message: ME
- Caesar values:

$$\text{M} = 12, \quad \text{E} = 04$$

Step 2: Encryption Formula
The encryption formula for RSA is:

$$C \equiv M^e \pmod{n}$$

where:
- M is the plaintext number,
- e is the encryption exponent,
- n is the modulus.

Step 3: Encrypt $M = 12$
Compute:

$$C_M \equiv 12^{41} \pmod{899}$$

Break 50 into binary:

$$41 = 101001_2 = 32 + 8 + 1$$

Thus:

$$12^{41} = 12^{32} \times 12^8 \times 12^1$$

Repeated squaring:

Power	Result $\pmod{899}$
12^1	12
12^2	$144 \equiv 144 \pmod{899}$
12^4	$144^2 = 20736 \equiv 59 \pmod{899}$
12^8	$59^2 = 3481 \equiv 784 \pmod{899}$
12^{16}	$784^2 = 614656 \equiv 639 \pmod{899}$
12^{32}	$639^2 = 408321 \equiv 175 \pmod{899}$

Now multiply the relevant powers:

$$C_M \equiv 175 \times 784 \times 12 \pmod{899}$$

$$175 \times 784 = 137200 \equiv 552 \pmod{899}$$

$$552 \times 12 = 6624 \equiv 331 \pmod{899}$$

$$\boxed{C_M = 331}$$

Step 4: Encrypt $E = 4$
Final Answer: Encrypted Message

Letter	Plaintext (ASCII)	Ciphertext
H	72	1177
I	73	1034

The encrypted message HI is:

$$\boxed{(1177, 1034)}$$

Properties of the encryption/decryption keys for RSA systems

In the RSA cryptosystem, the **encryption key** is given as:

$$(n, e),$$

where:
- $n = p \times q$, with p and q being large distinct prime numbers,
- e is the public exponent, chosen such that:

$$\gcd(e, \varphi(n)) = 1,$$

- $\varphi(n) = (p-1)(q-1)$ is Euler's totient function.

Condition for Determining the Decryption Key d:
The decryption key d is defined as the modular inverse of e modulo $\varphi(n)$. In other words, d satisfies the congruence:

$$d \cdot e \equiv 1 \pmod{\varphi(n)}.$$

This can also be written as:

$$d = e^{-1} \pmod{\varphi(n)}.$$

Summary of the steps:
1. Select two large prime numbers p and q.
2. Compute $n = p \times q$.
3. Compute $\varphi(n) = (p-1)(q-1)$.
4. Choose e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
5. Find d such that:

$$e \cdot d \equiv 1 \pmod{\varphi(n)}.$$

The value of d can be computed using the **Extended Euclidean Algorithm**.

3. Determine the block size for the RSA encryption.

Encryption key:

$$(p \times q, \; e)$$

$$\gcd(e, p \times q) = 1$$

$$n = p \times q = pq$$

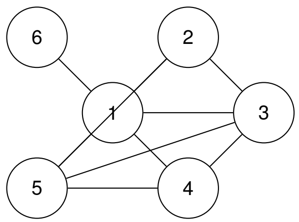
$$\text{Number of bits} = \lfloor \log_2(pq) \rfloor + 1$$

$$\text{Block size} = (\text{Number of bits}/8)\text{bytes}$$

$$c = m^e \mod (p \times q)$$

Solution to Problem 4

(1) Graph Diagram of G:



(2) Degrees of Vertices 2 and 5:

Vertex	Degree
2	3
5	5

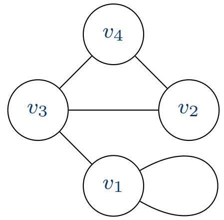
E.G. Problem 5

Given Incident Matrix:

$$M = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Explanation:
- **Rows = Vertices:** v_1, v_2, v_3, v_4
- **Columns = Edges:** e_1, e_2, e_3, e_4, e_5
- An entry of 1 in the matrix indicates that the vertex (row) is incident to the edge (column).

(1) Graph Diagram of G:



(2) Adjacency Matrix of G:

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Note: Entry $A_{11} = 1$ indicates the self-loop at vertex v_1. and G is **not** a simple graph because there is a self-loop at vertex v_1 (edge e_5).

Boolean function

Given the Boolean function:

$$F(x, y, z) = xy + y\bar{z} + z\bar{x}$$

(1) Sum-of-Product (SOP) Expansion

We first create the truth table for all possible values of x, y, z:

x	y	z	xy	$y\bar{z}$	$z\bar{x}$	$F(x,y,z)$
0	0	0	0	0	0	0
0	0	1	0	0	1	1
0	1	0	0	1	0	1
0	1	1	0	0	1	1
1	0	0	0	0	0	0
1	0	1	0	0	0	0
1	1	0	1	1	0	1
1	1	1	1	0	0	1

From the truth table, $F(x, y, z) = 1$ for the following input combinations:

$$(0, 0, 1), \; (0, 1, 0), \; (0, 1, 1), \; (1, 1, 0), \; (1, 1, 1)$$

The corresponding minterms (sum-of-products terms) are:

$$\bar{x}\bar{y}z \quad \text{for } (0, 0, 1),$$
$$\bar{x}y\bar{z} \quad \text{for } (0, 1, 0),$$
$$\bar{x}yz \quad \text{for } (0, 1, 1),$$
$$xy\bar{z} \quad \text{for } (1, 1, 0),$$
$$xyz \quad \text{for } (1, 1, 1).$$

Therefore, the sum-of-product expansion is:

$$F(x, y, z) = \bar{x}\bar{y}z + \bar{x}y\bar{z} + \bar{x}yz + xy\bar{z} + xyz.$$

(2) All Possible Triples (x, y, z) for which $F(x, y, z) = 1$:

The triples where the output is 1 are:

$$(0, 0, 1), \; (0, 1, 0), \; (0, 1, 1), \; (1, 1, 0), \; (1, 1, 1).$$

Boolean function 2

Given Truth Table:

x	y	$F(x,y)$
0	0	1
0	1	1
1	0	1
1	1	0

(1) Sum-of-Product (SOP) Expansion

From the truth table, $F(x, y) = 1$ for the following input combinations:
- $(0, 0) \to \bar{x}\bar{y}$
- $(0, 1) \to \bar{x}y$
- $(1, 0) \to x\bar{y}$

Thus, the SOP expression is:

$$F(x, y) = \bar{x}\bar{y} + \bar{x}y + x\bar{y}$$

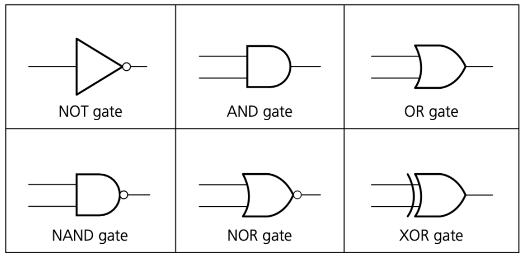
This can also be simplified using Boolean algebra:

$$F(x, y) = \bar{x} + \bar{y}$$

(because $\bar{x}\bar{y} + \bar{x}y = \bar{x}$ and $\bar{x} + x\bar{y} = \bar{x} + \bar{y}$).

(2) Circuit Diagram

Simplified expression: $F(x, y) = \bar{x} + \bar{y}$



x	y	AND	OR	$NAND$	NOR	XOR
0	0	0	0	1	1	0
0	1	0	1	1	0	1
1	0	0	1	1	0	1
1	1	1	1	0	0	0

12.

In each of the following alternatives, specify the induction hypothesis in the proof by induction on n that every positive integer n is a product of primes:

(a) **Using mathematical induction**

- **Base case:** $P(2)$: 2 is prime, so $P(2)$ is true.
- **Assume :** $P(2), P(3), \ldots, P(k)$ are all true, meaning each of these numbers is a product of primes.
- **Induction:** $P(k) \to k$ is a product of primes.
- **wts:** $P(k+1)$ is also true
  - **Case I:** $k+1$ is prime, then$k+1$ is product of primes.
  - **Case II:** If $k+1$ is not prime, then $k+1 = a \cdot b$, where $2 \leq a, b \leq k$. Then a and b can be written as a prove of prime

Part2

Let x be a real number in the open interval $(-1, 0)$. Prove using mathematical induction that for any positive integer

$$n > 1, (1+x)^n > 1 + nx.$$

Let $P(k)$ be the statement:

$$(1+x) > 1 + kx, \quad \text{for } k > 1, \ k \in \mathbb{Z}^+.$$

Theorem. Let $x \in (-1, 0)$ be a real number. Then for any integer $n > 1$,

$$(1+x)^n > 1 + nx.$$

STEP1 $P(n)$ is true for all n
STEP2 Prove $\forall n \in \mathbb{Z}^+$.
STEP3 Base Case: $n = 2$. Substitute $n = 2$ into the inequality:
Since $x \in (-1, 0)$, we have $x^2 > 0$. Thus,
Therefore, the base case holds.
STEP4 We show that the conditional statement

$$\forall n > 1[P(2) \wedge P(3) \wedge \cdots \wedge P(n)] \to P(n+1)$$

is true for all positive integers n.
Induction Hypothesis: Assume that for some integer $k \geq 2$, the inequality holds:

$$(1+x)^k > 1 + kx.$$

Inductive Step: We need to show that:

$$(1+x)^{k+1} > 1 + (k+1)x.$$

Observe that:

$$(1+x)^{k+1} = (1+x)^k (1+x).$$

By the induction hypothesis:

$$(1+x)^k > 1 + kx.$$

Substituting this into the expression for $(1+x)^{k+1}$:

$$(1+x)^{k+1} > (1+kx)(1+x).$$

Now expand the right-hand side:

$$(1+kx)(1+x) = 1 + x + kx + kx^2 = 1 + (k+1)x + kx^2.$$

Since $x \in (-1, 0)$, we have $x^2 > 0$, so $kx^2 > 0$ for $k \geq 2$.
Therefore:

$$1 + (k+1)x + kx^2 > 1 + (k+1)x.$$

This shows:

$$(1+x)^{k+1} > 1 + (k+1)x.$$

Conclusion: By the principle of mathematical induction, the inequality

$$(1+x)^n > 1 + nx$$

holds for all integers $n > 1$, where $x \in (-1, 0)$. ■

RSA Decryption Process

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Step 1: RSA Setup

- Public key: $n = 29 \times 31 = 899, \ e = 41$
- Message: `ME`
- Caesar values:

$$\text{M} = 12, \quad \text{E} = 04$$

Step 2: Encryption Formula
The encryption formula for RSA is:

$$C \equiv M^e \pmod{n}$$

where:

- M is the plaintext number,
- e is the encryption exponent,
- n is the modulus.

Step 3: Encrypt $M = 12$
Compute:

$$C_M \equiv 12^{41} \pmod{899}$$

Break 50 into binary:

$$41 = 101001_2 = 32 + 8 + 1$$

Thus:

$$12^{41} = 12^{32} \times 12^8 \times 12^1$$

Repeated squaring:

Power	Result $\pmod{899}$
12^1	12
12^2	$144 \equiv 144 \pmod{899}$
12^4	$144^2 = 20736 \equiv 59 \pmod{899}$
12^8	$59^2 = 3481 \equiv 784 \pmod{899}$
12^{16}	$784^2 = 614656 \equiv 639 \pmod{899}$
12^{32}	$639^2 = 408321 \equiv 175 \pmod{899}$

Now multiply the relevant powers:

$$C_M \equiv 175 \times 784 \times 12 \pmod{899}$$

$$175 \times 784 = 137200 \equiv 552 \pmod{899}$$

$$552 \times 12 = 6624 \equiv 331 \pmod{899}$$

$$\boxed{C_M = 331}$$

Step 4: Encrypt $E = 4$
Final Answer: Encrypted Message

Letter	Plaintext (ASCII)	Ciphertext
H	72	1177
I	73	1034

The encrypted message `HI` is:

$$\boxed{(1177, 1034)}$$

UK Traffic Light System Using Gray Code Sequence

Counting Sequences

- **Standard Binary Count:** 00 → 01 → 10 → 11
- **Gray Code Sequence:** 00 → 01 → 11 → 10

Inputs and Outputs

- **Inputs:**
  - J: First control switch (bit 1)
  - K: Second control switch (bit 2)
- **Outputs (Traffic Light Signals):**
  - X: Red light
  - Y: Amber (Yellow) light
  - Z: Green light

Gray Code Sequence: 00 → 01 → 11 → 10 **Inputs:** J, K
Outputs: X (Red), Y (Amber), Z (Green)

J	K	X (Red)	Y (Amber)	Z (Green)
0	0	1	0	0
0	1	1	1	0
1	1	0	0	1
1	0	0	1	0

Boolean Expressions

$$X = J'$$

$$Y = J \oplus K$$

$$Z = JK$$

- J' is the NOT of J
- $J \oplus K$ is the XOR of J and K
- JK is the AND of J and K