TERNA ENGINEERING COLLEGE, NERUL
Department of Computer Engineering

Cryptography and System Security (CSS)

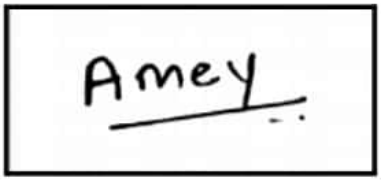
Assignment No 1

Sr. No	Question	CO -mapped
Q. 1	Define Security goals, Services, Mechanisms with example and how each one can be achieved.	(CO-1)
Q. 2	Explain Substitution and transposition techniques, Vigenere cipher, Playfair cipher, Hill cipher with example.	(CO-1)
Q. 3	Explain Chinese Remainder theorem with example	(CO-2)
Q. 4	Explain the Euclid Algorithm, Fermat/Euler Algorithm	(CO-2)
Q. 5	A and B decide to use a Diffie Hellman key exchange algorithm. They choose p= 23 and g=5 as public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share.	(CO-3)
Q. 6	Explain the RSA algorithm with an example.	(CO-3)

CSS ASSIGNMENT - 1

AMEY THAKUR

COMPS TE B-50



AMEY TE B 50 Amey

PAGE No.
DATE / /

Q.1 Define Security goals, Services, Mechanisms with example and how each one can be achieved.

Ans:

Providing security to the information assets of our modern age has become a matter of supreme importance. The three main goals associated with security are :

(i) Confidentiality
(ii) Integrity
(iii) Availability

(i) Confidentiality :

- It is a common aspect of information security. We need to protect our confidential information from getting leaked into public.
- For eg. in military, confidentiality is related to national security. In business, certain information always needs to be hidden from competitors.
- It applies to both the storage of information as well as for transmission of information.

(ii) Integrity :

- In information security, integrity means maintaining and assuring accuracy and completion of data over its entire life-cycle.
- It means that changes can be done only by authorized entities and only through authorized mechanism.
- Securing integrity of data is extremely important E.g. You are sending Rs 1000, somebody tampers with the integrity of transactions and actually sends Rs. 100000.

AMEY TE B 50 Amey

PAGE No. 1
DATE / /

- Data can also be lost dye to natural reasons like power outage, floods etc.

(iii) Availability

- Availability of information refers to ensuring that authorized entities get information when needed
- An information which is stored and maintained is useless if it's not available when needed.
- Denying access to the information has become a popular mode of cyber attack.
  Eg. DDos (Distributed Denial of Service)

Mechanisms to achieve the above goals are :

(i) Confidentiality
- Encipherment
- Routing Control.

(ii) Integrity
- Encipherment
- Digital Signature
- Data Integrity

(iii) Availability
- Creating backups
- Routing Control

AMEY TE B 50 Amey

PAGE No.
DATE / /

Q.2 Explain Substitution and Transposition Technique, Vigenere cipher, Playfair Cipher, Hill Cipher with example.

Ans:

Substitution Technique:

It is a technique in which each letter or bit of the plaintext is substituted or replace by some other letter, number or symbol to produce ciphertext. Substitution means replacing an alphabet of plaintext with an alphabet of ciphertext.

Playfair Cipher:

It is multiple letter encryption technique which uses 5 * 5 marine table to store the letters of the phrase given for encryption which letter on becomes key for encryption and decryption. eg. Keyword is FAIR EXAMPLE

Hill Cipher:

- It is a polygraphic substitution cipher based on Linear Algebra.
- Each letter is represented by a number modulo 26. Often the simple scheme (A = 0, B = 1, C = 2, ..., Z = 25) is used, but this is not an essential feature of the cipher.
- To encrypt a plaintext message, each block is multiplied by an invertible m * m matrix, each block is multiplied by the inverse of the matrix used for encryption.

AMEY TE B 50 Amey

PAGE No. / DATE / /

The technique can be described as following:

$$C_{i1} = (K_{11} P_{i1} + K_{12} P_{i2} + K_{13} P_{i3}) \bmod 26$$
$$C_{i2} = (K_{21} P_{i1} + K_{22} P_{i2} + K_{23} P_{i3}) \bmod 26$$
$$C_{i3} = (K_{31} P_{i1} + K_{32} P_{i2} + K_{33} P_{i3}) \bmod 26$$

This technique uses column vector and matrices:

$$\begin{bmatrix} C_{i1} \\ C_{i2} \\ C_{i3} \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{bmatrix} P_{i1} \\ P_{i2} \\ P_{i3} \end{bmatrix} \bmod 26$$

Example: Encrypt the message "Exam" using the Hill cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

Solution: Key (K) = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

Plaintext (P_i) = "Exam"

$$C_i = KP_i \bmod 26 \quad \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \times \begin{bmatrix} 4 & 23 \\ 0 & 12 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 151 & 167 \\ 60 & 84 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 21 & 11 \\ 8 & 6 \end{bmatrix}$$

= VLIG

AMEY TE B 50 Amey

PAGE No.
DATE / /

Vigenere Cipher :

This is a method of encryption alphabetic text. It uses a simple form of polyalphabetic.

- A polyalphabetic cipher is any cipher based on substitution using multiple substition alphabets. The encryption of the original text is done using the vigenere square or vigenere table.
- The table consists of the alphabet written out 26 times in different rows, each alphabets shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caeser Ciphers.
- At different points in the encryption procees the cipher uses a different alphabet from one of the rows.
- The alphabet used at each point depends on a repeating keyword.

Formula of encryption :

$$E_i = (P_i + K_i) \bmod 26$$

Formula of decryption :

$$D_i = (E_i - K_i) \bmod 26$$

where, E ⇒ Encryption
D ⇒ Decryption
P ⇒ Plaintext
K ⇒ Key

AMEY TE B 50 Amey

PAGE No.
DATE / /

A	00
B	01
C	02
D	03
E	04
F	05
G	06
H	07
I	08
J	09
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

Example:

Plaintext = AMEY

KEY = MEGA

Plaintext	A	M	E	Y
Value (P)	00	12	04	24
Key	M	E	G	A
Value (K)	12	04	06	00
Ciphertext Value(E)	12	16	10	24
Ciphertext	M	Q	K	Y

Ciphertext	M	Q	K	Y
(E)	12	16	10	24
key	M	E	G	A
(K)	12	04	06	00
(P)	00	12	04	24
Plaintext	A	M	E	Y

AMEY TE B 50 Amey

PAGE No.
DATE / /

Q.3 Explain Chinese Remainder Theorem with example.

Ans:

The Chinese Remainder Theorem.

If $m_1, m_2, \ldots, m_k$ are pairwise relatively prime positive integers and if $a_1, a_2, \ldots, a_k$ are any integers, then the simultaneous congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_k \pmod{m_k}$$

and the solution is unique modulo m, where $m = m_1 m_2 \ldots m_k$

Proof:

To keep the notation simpler, we will assume $k = 4$. Note that proof is constructive. i.e. it shows us how to actually construct a solution.

Our simultaneous congruences are:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$x \equiv a_3 \pmod{m_3}$$
$$x \equiv a_4 \pmod{m_4}$$

AMEY TE B 50 Amey

PAGE No. / DATE / /

Our goal is to find integers w_1, w_2, w_3, w_4 such that:

	Value mod m_1	Value mod m_2	Value mod m_3	Value mod m_4
w_1	1	0	0	0
w_2	0	1	0	0
w_3	0	0	1	0
w_4	0	0	0	1

Once we have found w_1, w_2, w_3, w_4, it is easy to construct x:

$x = a_1 w_1 + a_2 w_2 + a_3 w_3 + a_4 w_4$

Moreover, as long as the moduli (m_1, m_2, m_3, m_4) remain the same, we can use the same w_1, w_2, w_3, w_4 with any a_1, a_2, a_3, a_4.

First define:

$Z_1 = m / m_1 = m_2 m_3 m_4$

$Z_2 = m / m_2 = m_1 m_3 m_4$

$Z_3 = m / m_3 = m_1 m_2 m_4$

$Z_4 = m / m_4 = m_1 m_2 m_3$

Note that

① $Z_i \equiv 0 \pmod{m_j}$ for $j = 2, 3, 4$.

② $\gcd(Z_1, m_1) = 1$ (If a prime p dividing m_1 also divides $Z_1 = m_2 m_3 m_4$, then p divides m_2, m_3, m_4)

and likewise for Z_2, Z_3, Z_4.

Next define:

$$y_1 \equiv z_1^{-1} \pmod{m_1}$$
$$y_2 \equiv z_2^{-1} \pmod{m_2}$$
$$y_3 \equiv z_3^{-1} \pmod{m_3}$$
$$y_4 \equiv z_4^{-1} \pmod{m_4}$$

The inverses exist by ② above, and we can find them by Euclid's extended algorithm.

Note that:

③ $y_i z_i \equiv 0 \pmod{m_j}$ for $j = 2,3,4$.
(Recall $z_i \equiv 0 \pmod{m_j}$)

④ $y_i z_i \equiv 1 \pmod{m_i}$

and likewise for $y_2 z_2$, $y_3 z_3$, $y_4 z_4$.

Lastly define:

$$w_1 \equiv y_1 z_1 \pmod{m}$$
$$w_2 \equiv y_2 z_2 \pmod{m}$$
$$w_3 \equiv y_3 z_3 \pmod{m}$$
$$w_4 \equiv y_4 z_4 \pmod{m}$$

Then w_1, w_2, w_3, w_4 have the properties in the table above.

AMEY TE B 50 Amey

PAGE No. / DATE / /

Example: Find all solutions of $x^2 \equiv 1 \pmod{144}$

Soln:

$144 = 16 \cdot 9 = 2^4 3^2$ and $\gcd(16, 9) = 1$

We can replace our congruence by two simultaneous congruences:

$x^2 \equiv 1 \pmod{16}$ and $x^2 \equiv 1 \pmod{9}$

There are 8 alternatives:

① $x \equiv 1 \pmod{16}$ and $x \equiv 1 \pmod{9}$

② $x \equiv 1 \pmod{16}$ and $x \equiv -1 \pmod{9}$

③ $x \equiv -1 \pmod{16}$ and $x \equiv 1 \pmod{9}$

④ $x \equiv -1 \pmod{16}$ and $x \equiv -1 \pmod{9}$

⑤ $x \equiv 7 \pmod{16}$ and $x \equiv 1 \pmod{9}$

⑥ $x \equiv 7 \pmod{16}$ and $x \equiv -1 \pmod{9}$

⑦ $x \equiv -7 \pmod{16}$ and $x \equiv 1 \pmod{9}$

⑧ $x \equiv -7 \pmod{16}$ and $x \equiv -1 \pmod{9}$

By the chinese remainder theorem with $k = 2$, $m_1 = 16$ and $m_2 = 9$

Each case above has a unique soln for x modulo 144.

We compute:

$z_1 = m_2 = 9$ $\quad$ $z_2 = m_1 = 16$

$y_1 \equiv 9^{-1} \equiv 9 \pmod{16}$ $\quad$ $y_2 \equiv 16^{-1} \equiv 4 \pmod{9}$

$w_1 \equiv 9 \cdot 9 = 81 \pmod{144}$ $\quad$ $w_2 \equiv 16 \cdot 4 \equiv 64 \pmod{144}$

AMEY TE B 50 Amey

PAGE No.
DATE / /

The 8 solutions are:

① $x \equiv 1 \cdot 81 + 1 \cdot 64 \equiv 145 \equiv 1 \pmod{144}$

② $x \equiv 1 \cdot 81 + (-1) \cdot 64 \equiv 17 \equiv 17 \pmod{144}$

③ $x \equiv (-1) \cdot 81 + 1 \cdot 64 \equiv -17 \equiv -17 \pmod{144}$

④ $x \equiv (-1) \cdot 81 + (-1) \cdot 64 \equiv -145 \equiv -1 \pmod{144}$

⑤ $x \equiv 7 \cdot 81 + 1 \cdot 64 \equiv 631 \equiv 55 \pmod{144}$

⑥ $x \equiv 7 \cdot 81 + (-1) \cdot 64 \equiv 503 \equiv 71 \pmod{144}$

⑦ $x \equiv (-7) \cdot 81 + 1 \cdot 64 \equiv -503 \equiv -71 \pmod{144}$

⑧ $x \equiv (-7) \cdot 81 + (-1) \cdot 64 \equiv -603 \equiv -55 \pmod{144}$

AMEY TE B 50 Amey

PAGE No. DATE / /

Q.4. Explain the Euclid Algorithm, Fermat / Euler Algorithm.

Ans:

Euclid Algorithm:

- The Euclidean algorithm is a technique for quickly finding the GCD of two integer.
- The Eucladean algorithm for finding out GCD (A, B) is as follows:
- If A = 0 then GCD (A, B) = B.
  ∵ GCD (0, B) = B and we can stop
- If B = 0 then GCD (A, B) = A.
  ∵ GCD (A, 0) = A and we can stop.
- Write A in qotient remainder form
  (A = B · Q + B)
- Find GCD (B, R) using the Euclidean algorithm since GCD (A, B) = GCD (B, R)

Example : Find the GCD of 270 & 192

A = 270 A ≠ 0

B = 192 B ≠ 0

Use long division to find that 270/192 = 1 with a remainder of 78.

270 = 192 * 1 + 78

Find GCD (192, 78) since GCD (270, 192) = GCD. (192, 78)

A = 192 B = 78

A ≠ 0 B ≠ 0

AMEY TE B 50 Amey

PAGE No.
DATE 1/ /

Use long division to find that 192/78 = 2 with a remainder of 36.

192 = 78 * 2 + 36

Find GCD (192, 78) since GCD(192, 78) = GCD(78, 36)

A = 78 A ≠ 0

B = 36 B ≠ 0

Use long division to find that 78/36 = 2 with a remainder of 6.

We can write this as:

78 = 36 * 2 + 6

Find GCD (36, 6), since GCD(78, 36) = GCD(36, 6)

A = 36 A ≠ 0

B = 6 B ≠ 0

Use long division to find that 36/6 = 6 with a remainder of 0.

36 = 6 * 6 + 0

Find GCD(6, 0), since GCD(36, 6) = GCD(6, 0).

A = 6 A ≠ 0

B = 0 B = 0 GCD(6, 0) = 6

AMEY TE B 50 Amey

PAGE No.
DATE / /

GCD (270, 192)
= GCD (192, 78)
= GCD (78, 36)
= GCD (36, 6)
= GCD (6, 0)
= 6

∴ GCD (270, 192) = 6

Euler's Theorem:

It states that for every a & n that are relatively prime:

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

Example:

a = 3
n = 10
$\phi(n) = ?$

Let $\phi(n) = \phi(10) = \{1, 3, 7, 9\} = 4$

According to Euler's Theorem.

$3^4 = 1 \pmod{10}$
$3^4 = 1 \mod 10$
$81 = 1 \mod 10$ (81 mod 10
= 1 ∠ 1 mod 10
= 1)

Hence Proved

AMEY TE B 50 Amey

PAGE No.
DATE / /

Fermat Theorem

Fermat Theorem plays an important role in public key cryptography

Theorem:

- For a prime number p, a is an integer which is not divisible by p then,

$$a^{p-1} \pmod p$$

A variant of this theorem is

If p is a prime and a is a coprime to p. (i.e GCD (a, p) = 1) then,

$$a^p \equiv a \pmod p$$

- Basically this theorem is useful in public key RSA and primarily testing
- Let us have $a = 3$ & $p = 5$. then as per the above theorem we have $3^{5-1} = 3^4 = 81 = 1 \pmod 5$

Since, on dividing 81 with 5, we have remainder 1.

Hence Proved

AMEY TE B 50 Amey

PAGE No.
DATE / /

Q.5.

Ans:

A chooses $x_A = 16$

B chooses $x_B = 15$

A's public key using its secret key

$y_A = g^{x_A} \bmod p.$

$y_A = 5^6 \bmod 23 = [(5^2 \bmod 23) * (5^2 \bmod 23) * (5^2 \bmod 23)] \bmod 23$

$y_A = [2 * 2 * 2] \bmod 23$

$y_A = 8$

B's public key using its secret key

$y_B = g^{x_B} \bmod p.$

$y_B = 5^{15} \bmod 23 = [(5^6 \bmod 23) * (5^6 \bmod 23) * (5^3 \bmod 23)] \bmod$

$y_B = [8 * 8 * 8] \bmod 23$

$y_B = 19$

The above 2 public keys are exchanged by both A & B.

Session keys.

A will compute key using B's public key

$K_{AB} = y^{x_{BA}} \bmod p.$

$= 19^6 \bmod 23$

$= [(19^2 \bmod 23) * (19^2 \bmod 23) * (19^2 \bmod 23)] \bmod$

$= 2$

AMEY TE B 50 Amey

PAGE No.
DATE / /

B will compute key using A's public key

$K_{BA} = y^{x_A{}^B} \bmod p$

$= 8^{15} \bmod 23$

$= [(8^6 \bmod 23) * (8^6 \bmod 23) * (8^3 \bmod 23)] \bmod 23$

$= 2$

$\therefore K_{AB} = 2$ & $K_{BA} = 2$.

AMEY TE B 50 Amey

PAGE No.
DATE / /

Q.6. Explain RSA algorithm with example.

Ans:

① Most widely accepted and implemented general purpose approach to public key encryption developed by Rivest - Shamir and Adleman (RSA) at MIT university.

② RSA scheme is block cipher in which the plaintext and ciphertext are integers between 0 and $n-1$ for some n.

③ Typical size of n is 1024 bits.
i.e. $n < 2$.

④ Description of Algorithm

- The scheme developed by Rivest, Shamir and Adleman makes use of an expression with exponentials.
- Plaintext is encrypted in block having a binary value than some number n.
- Block size $\leq \log_2(n)$
  If block size = i bits then,
  $2^i \leq n \leq 2^i + 1$
- Encryption and decryption are of the following form for some plaintext M and ciphertext C.

$$C = M^e \bmod n$$
$$M = C^d \bmod n$$
$$M = (M^e)^d \bmod n$$
$$M = M^{ed} \bmod n.$$

- Both sender and receiver must know the value of n.
- The sender knows the value of e, and only the receiver knows the value of d.

AMEY TE B 50 Amey

PAGE No.
DATE / /

- Thus this is a public key encryption algorithm with a public key of PU = {e, n} and private key of PR = {d, n}

⑤ RSA Algorithm

a) Key generation:
- Select p, q ... p & q both are the prime numbers. p ≠ q.
- Calculate n = p × q
- Calculate φ(n) = (p-1) (q-1)
- Select integer ... gcd (d (φ(n), e)) = 1 & 1 < e < φ(n)
- Calculate d ; d = e⁻¹ mod (n)
- Public key PU = {e, n}
- Private key, PR = {d, n}

b) Encryption
- Plaintext : m < n < p = "M"
- Ciphertext : C

c) Decryption
- Ciphertext : C
- Plaintext : M = C^d mod n
- Note 1 : φ(n) → Euler's Totients function
- Note 2 : Relationship between e and d

ed (mod (φ(n))) = 1

ed = 1 mod (φ(n))

d = e⁻¹ mod (φ(n))

AMEY TE B 50 Amey

PAGE No.
DATE / /

⑤ Example:

Key generation:

① Select 2 prime numbers → p = 17 & q = 11

② Calculate n = p × q = 17 × 11 = 187

③ Calculate = 16 × 10 = 160

Select 'e' such that e is relatively prime to (n) = 160 and e <

④ Determine d such that

de = 1 mod (n)

d × 7 = 1 mod 160

↓

161

d = e^{-1} mod (n) [161 / 7 = div. [d] 23 + 1]

d = 23

remainder = 1

Then the resulting keys are public keys

PU = {7, 187}

PR = {23, 187}

Let M = 88 for encryption

C = 88^7 mod (187) 88 mod 187

= 88 88^2 mod 187

= 7744 mod 187

= 59969536 mod 187 = 132

AMEY TE B 5⁰ Amey

PAGE No. DATE / /

$88^7 \mod 187$

$= (88^4 \mod 187) \times (88^2 \mod 187) \times (88 \mod 187) \mod 187$

$= (132 \times 77 \times 88) \mod 187$

$= 894432 \mod 187$

$= 11$

- For Decryption :

$M = C^d \mod 187$

$= 11^{23} \mod 187$ $\quad 11^1 \mod 187 = 11$ $\quad 11^2 \mod 187 = 121$

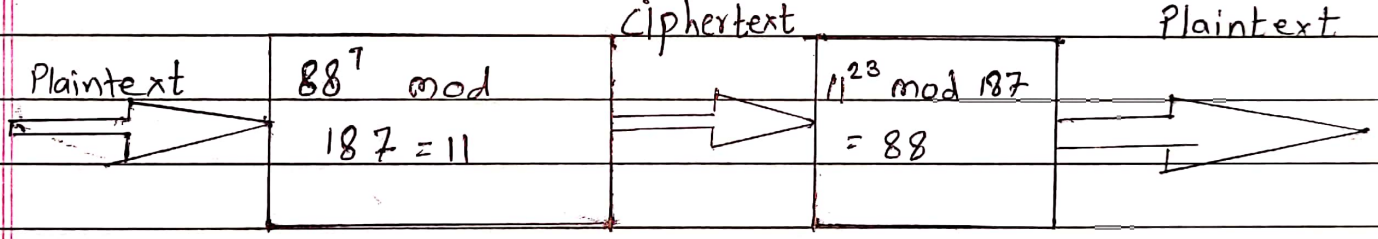
$= 11^4 \mod 187$

$= 14641 / 187$

$= 55$

$= (11^8 \mod 187 \times 11^8 \mod 187 \times 11^4 \mod 187 \times 11^2 \mod 187 \times 11^1 \mod 187) \mod 187$

$= (33 \times 33 \times 55 \times 81 \times 11) \mod 18$



Encryption
PU = {7, 187}

Decryption
PR(823187)