(IT-2|010) [EID Holiday Assignment]

Q1] Prove Fermat's Little Theorem and use it to compute $a^{p-1} \bmod p$ for given values of $a=7$, $p=13$. Then discuss how this theorem is useful in cryptographic algorithms like RSA.

⇒ The statement of Fermat's little theorem (FLT) is If p is a prime number and a is any integer not divisible by p, then $a^{p-1} \equiv 1 \pmod p$

Now here its proof:

Let a be an integer such that $\gcd(a,p)=1$, and let us consider the set of integers:

$$S = \{1, 2, 3, \ldots, p-1\}$$

Multiplying each element of this set by a modulo p we get $a.S = \{a.1, a.2, \ldots a.(p-1)\} \bmod p$

Since a is invertible mod p, all $a.i \bmod p$ are distinct and non-zero. so this new set is just a permutation of S.

Taking the product of all elements in both sets

$$a^{p-1}.(1.2.\ldots.(p-1)) \equiv (1.2.\ldots.(p-1)) \bmod p$$

by canceling the factorial term we get

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

(IT-2020)

Now for the question apply $a=7$, $p=13$ since 13 in a prime and 7 in not divisible by 13: $a^{p-1} = 7^{13-1} = 7^{12}$

$$7^{12} \equiv 1 \bmod 13$$

$$7^{12} \bmod 13 = 1$$

Fermat's Little Theorem forms a foundation for modular arithmetic used in public-key cryptography. In RSA, IDEA relies on the difficulty of factoring large primes and properties of modular exponentiation. It can be used Encrypt/decrypt message by raising to a power mod a prime. Generate keys, since modular inverses depend on this idea. Key use cases

1) Fast modular exponentiation
2) Verifying primality of numbers
3) Computing modular inverses

(IT-21010)

Q2| Euler Tuotient Function: Compute $\phi(n)$ for $n = 35, 95, 100$. Prove that if a and n are coprime, then $a^{\phi(n)} \equiv 1 \bmod n$

⇒ Definition: $\phi(n)$ is the number of integers less then or equal to n that are coprime to n. If $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$, then $\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$

Now compute for $\phi(n)$ for given values:

1. $n = 35 = 5 \times 7$ $\quad \phi(35) = 35\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 24$
2. $n = 95 = 3^2 \times 5$ $\quad \phi(95) = 95\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 24$
3. $n = 100 = 2^2 \times 5^2$ $\quad \phi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40$

Now we know the Euler's theorem is

If a and n are coprime, then $a^{\phi(n)} \equiv 1 \bmod n$

Let $R = \{r_1, r_2 \ldots r_{\phi(n)}\}$ be the set of positive integers less than n that are coprime to n. Multiplying each by a, we get: $a.R = \{ar_1, ar_2, \ldots, ar_{\phi(n)}\} \bmod n$

Because $\gcd(a,n) = 1$, this new set is just a permutation of R. So $a^{\phi(n)} \cdot (r_1 \cdot r_2 \cdots r_{\phi(n)}) \equiv (r_1 \cdot r_2 \cdots r_{\phi(n)}) \bmod n$

canceling both side $a^{\phi(n)} \equiv 1 \bmod n$ (Proved)

(IT-2101)

Q3] Solve the system of congruences using the Chinese Remainder Theorem and Prove that x congruent to 11 on mod $N = 3 \times 4 \times 5 = 60$.

$x \equiv 2 \bmod 3 \quad x \equiv 3 \bmod 4 \quad x \equiv 1 \bmod 5$

⇒ We are given the system of congruences:

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 4 \\ x \equiv 1 \bmod 5 \end{cases}$$

we are to solve this using the Chinese Remainder Theorem and show that the solution

$$x \equiv 11 \bmod 60$$

$n_1 = 3, \quad n_2 = 4, \quad n_3 = 5$

$N = n_1 \cdot n_2 \cdot n_3 = 60$

$N_1 = N/n_1 = 60/3 = 20$

$N_2 = N/n_2 = 60/4 = 15$

$N_3 = N/n_3 = 60/5 = 12$

we find modular inverses. We want:

M_1 such that $20 \cdot M_1 \equiv 1 \bmod 3 \Rightarrow M_1 = 2$

because $20 \cdot 2 = 40 \equiv 1 \bmod 3$

(IT-2010)

M_2 such that $15 \cdot M_2 \equiv 1 \bmod 4 \Rightarrow M_2 = 3$ because $15 \cdot 3 = 45 \equiv 1 \bmod 4$. M_3 such that $12 \cdot M_3 \equiv 1 \bmod 5 \Rightarrow M_3 = 3$ because $12 \cdot 3 = 36 \equiv 1 \bmod 5$

$$x = a_1 N_1 M_1 + a_2 N_2 M_2 + a_3 N_3 M_3 \bmod N$$

where: $a_1 = 2, a_2 = 3, a_3 = 1$

$$x = 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 1 \cdot 12 \cdot 3$$
$$= 80 + 135 + 36 = 251$$

$$x \equiv 251 \bmod 60 \Rightarrow x \equiv 11 \bmod 60$$

So finally $x \equiv 11 \bmod 60$

Q9) Find whether 561 is a Carmichael number by checking its divisibility and Fermat's test.

⇒ A Carmichael number is a composite number n such that $a^{n-1} \equiv 1 \bmod n$ for all integers a such that $\gcd(a, n) = 1$

561 is not prime. $561 = 3 \times 11 \times 17$

but it's composite number made of distinct primes.

(IT-21010)

A composite number n is a Carmichael if and only if: n is square-free and for every prime p dividing n, it holds that $p-1 \mid (n-1)$.

$n = 561$ so $n-1 = 560$

Prime factors: $p_1 = 3$, $p_2 = 11$, $p_3 = 17$

$3-1 = 2 \mid 560$

$11-1 = 10 \mid 560$

$17-1 = 16 \mid 560$

561 is square free and satisfies the above condition so we can say that 561 is a Carmichael number

Q5] Find a generator (primitive root) of the multiplicative group modulo 17.

⇒ A primitive root modulo p (where p is a prime) is an integer g such that

$g^1, g^2, \ldots, g^{p-1} \bmod p$

(IT-21010)

that in g is a generator of the multiplicative group modulo p.

Since 17 is prime, the multiplicative group modulo 17 has $\phi(17) = 16$ elements. we want to find an integer g such that,

$g^k \neq 1 \mod 17$ for all $1 < k < 16$, and $g^{16} \equiv 1 \mod 17$

To test if g is a primitive root modulo 17, we must ensure: $g^{16/d} \neq 1 \mod 17$ for all prime divisors d of 16. 16 : 2 so check

$g^{16/2} = g^8$, g^4 and g^2 (Since $16 = 2^4$)

Try $g = 3$ we found.

$3^2 = 9 \mod 17 \neq 1$, $3^4 = 81 \mod 17 = 13 \neq 1$

$3^8 = 13^2 = 169 \mod 17 = 16 \neq 1$, $3^{16} \mod 17 = 1$

So, 3 passes all the test. primitive root test

So, our answer is 3 is a primitive root modulo 17.

(IT-210)

Q6] Solve the discrete Logarithm Problem
Find x such that $3^x \equiv 13 \bmod 17$.

$\Rightarrow 3^x \equiv 13 \bmod 17$

Here Base $g = 3$, modulus $p = 17$

So result $3^x \equiv 13 \bmod 17$

we need to find the smallest positive integer x such that this is true

$3^1 \equiv 3 \bmod 17$ NO

$3^2 \equiv 9 \bmod 17$ NO

$3^3 \equiv 10 \bmod 17$ NO

$3^4 \equiv 13 \bmod 17$ Yes

So our answer is $x = 4$

$3^4 = 81 \equiv 13 \bmod 17$

(IT-21010)

Q7] Discuss the role of the discrete algorithm in the Diffie-Hellman key Exchange

⇒ The Diffie-Hellman key Exchange is a cryptographic protocol that allows two parties to securely generate a shared secret over a public channel. It relies on the difficulty of the discrete algorithm problem (DLP) the challenge of finding x given $g^x \bmod p$ where g is a known base and p is a prime.

In this protocol, both parties exchange values based on their private keys and a common base but an attacker cannot compute the shared secret without solving the discrete algorithm a task that is computationally hard for large primes. Thus the security of Diffie-Hellman fundamentally depends on the infeasibility of solving the discrete logarithm problem.

IT-2010

Q8] Here is the comparison of the substitution cipher Transposition cipher and playfair cipher based on encryption mechanism.

1) Encryption Mechanism

Substitution cipher replace each letter with another letter based on a fixed mapping

Transposition cipher rearrange the positions of characters without changing the actual letters

playfair cipher encrypts pairs of letters using a 5×5 matrix and specific rules.

2) Key Space

$26! = 4 \times 10^{26}$ for substitution cipher.

Transposition cipher depends on length for n letters $n!$ and playfair cipher is

$25! = 1.5 \times 10^{25}$

3) Vulnerability to frequency Analysis

Substitution cipher Highly vulnerable

Transposition cipher moderate,

playfair cipher less vulnerable

(IT-2010)

Now for example with plaintext: "HELLO"

Substitution Cipher: Alphabet Shifted by 3: A→D, B→E, ... X→A, Y→B, Z→C

Encryption: H→K, E→H, L→O, L→O, O→R

ciphertext: KHOOR

Transposition Cipher: Read column top to bottom

Column 1: HL, Column 2: EO, Column 3: L

ciphertext: HLEOL

playfair cipher: Prepare matrix:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Split plaintext into digraphs: HELLO → HE, LX

Encrypt using playfair rules:

HE → Find positions H(2,1), E(3,0) → rectangle rule → R

LX → L(0,0), X(0,3) → same row → P, Z

LO → L(0,0), O(0,1) → rectangle rule → P, V

ciphertext: FCPZPV

(IT-2010)

Q9] Affine cipher Encryption Function:

$E(x) = (a.x + b) \bmod 26$

$a = 5$, $b = 8$, plaintext "Dept of ICT, MBSTU

a) can Remove punctuation and space and convert all letters to uppercase

DEPTOFMBSTICTMBSTU

Letter to number mapping

A = 0, B = 1, ... Z = 25

For D $x = 3$ $E(3) = (5.3 + 8) \bmod 26 = 23 = X$

For E $x = 4$ $E(4) = (5.4 + 8) \bmod 26 = 2 = C$

For P $x = 15$ $E(15) = (5.15 + 8) \bmod 26 = 3 = D$

↓

By using this formula we get the Encrypted Text "XCDVAHWSVGNGVA"

b) Decryption function:

$D(y) = a^{-1}.(y - b) \bmod 26$

$a = 5$ Try multiplicative value

$5 \times 21 = 105 \equiv 1 \bmod 26$

So, $a^{-1} = 21$

(IT-2020)

Decrypt each letter using the function

For X $y = 23$ $21(23) \bmod 26 = 3 \Rightarrow D$

For C $y = 2$ $21(-6) = -126 \bmod 26 = 4 \Rightarrow E$

For D $y = 3$ $21(-5) = -105 \bmod 26 = 15 \Rightarrow P$

For V $y = 21$ $21(13) = 273 \bmod 26 = 11 \Rightarrow T$

So the Decrypted Text is

DEPTOFICTMBSTU

Q(b) SPHINX Cipher is a simple hybrid encryption method that combines both substitution and permutation techniques enhanced with a light-weight pseudo-random number generation (PRNG) seeded by a numeric keyphrase. Each letter of the plaintext (A-Z) with a shuffled alphabet. Then, the substituted text is divided into fixed-size blocks and each block undergoes a position-based permutation based on a PRNG-derived pattern. [2, 0, 9, 1, 3] for

(IT-2010)

instance, "HELLO" might be encrypted to SIGIS using this method;
Decryption reverses this process by first applying the inverse permutations to each block and then using the inverse of the substitution mapping. While this cipher offers better security than basic substitution or transposition alone - by disrupting both letter frequencies and positional patterns - it still has vulnerabilities. If the PRNG or key is weak or predictable, an attacker could negate the substitutions and permutations sequences. Additionally without block chaining or authentication repeated blocks produce repeated ciphertexts and are susceptible to known plaintext attacks.