Md. Uday Talukdar
17-21021

If p is a prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof

Multiplication by a non-zero number permutes the residues.

* Consider the set:

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

* Multiply each element by a:

$$a \cdot S = \{a \cdot 1, a \cdot 2, \ldots a \cdot (p-1)\}$$

* Because p is prime and $\gcd(a, p) = 1$ each element in $a \cdot S$ is distinct mod p and still covers all residues $1, 2 \ldots, p-1$ in some order.

Uday
IT-21021

So,

$$a \cdot 1 \cdot a \cdot 2 \cdot \cdots \cdot a \cdot (p-1) \equiv 1 \cdot 2 \cdot 1 \cdots (p-1) \pmod{p}$$

Since $(p-1)!$ is not zero mod p (its the product of numbers 1 to $p-1$), we can devide both sides:

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

Given

$a = 7$

$p = 13$

Then $7^{12} \equiv 1 \pmod{13}$.

So the result is:

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

Uday
IT-2102

It is useful in cryptography algorithm like RSA

- Fermat's little Theorem is a special case of Euler theorem; which says

$$a^{\phi(n)} \equiv 1 \pmod{n} \text{ if } \gcd(a,n) = 1$$

Here; for primes $\phi(p) = p-1$)

- RSA relies on modular exponentiation and the fact that we can compute the modular inverse of exponents. using Eular theorem.

- In RSA
  * You choose two larger prime p and q
  * Compute $n = pq$ and $\phi(n) = (p-1)(q-1)$

Udoy 1
It-2/021

The security depends on the fact that exponentiation and inverse modulo $\phi(n)$ work correctly

Encryption:

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

Decryption:

$$M \equiv C^d \pmod{n}, \text{ where } ed \equiv 1$$

Q2

Euler totient function

Compute $\phi(n)$ for

$$n = 35, 45, 100$$

Formula:

If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$

Then

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Uday
IT-21021

1) $n = 35$

$35 = 5 \times 7$

$\phi(35) = 35\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)$.

$= 35\left(\frac{4}{5}\right)\left(\frac{6}{7}\right)$

$= 35 \times \frac{24}{35}$

$= 24$

Ans

2) $n = 45$

~~$\phi(45) = 45\left(1-\right.$~~

$\phi(45) = 5 \times 3^2$

$\phi(45) = 45\left(1-\frac{1}{5}\right)\left(1-\frac{1}{3}\right.$

$= 45 \times \frac{4}{5} \times \frac{2}{3}$

$= 45 \times \frac{8}{15}$,

$= 24$.

Ans

Uday
I-192091

3) $n = 100$

$100 = 2^2 \times 5^2$

$$\phi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100 \times \frac{1}{2} \times \frac{1}{5}$$

$$= 100 \times \frac{4}{10}$$

$$= 40$$

Ans

Eular theorem

if $\gcd(a, n) = 1$, then

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

Uday
IT-21021

Q3

Given that,

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 4$
$x \equiv 1 \pmod 5$

Now $x \equiv 11 \pmod{60}$

$x \equiv 2 \pmod 3$

possible x: 2, 5, 8, 11

Next $x \equiv 3 \pmod 4$

2 mod 4 → 2 ⇒ no
5 mod 4 → 1 ⇒ no
8 mod 4 → 0 ⇒ no
11 mod 4 → 3 ⇒ yes

So, $x \equiv 11 \pmod{12}$ (LCM of 3 and 4)

Now add $x \equiv 1 \pmod 5$

possible:

11 mod 5 = 1 — Yes

So $x \equiv 11 \pmod{60}$

combined modulus is

$N = 3 \times 4 \times 5 = 60$

Thus $x \equiv 11 \pmod{60}$

94

Is 561 a carmichael number?

Definition:
A composite number n is a carmichael number if $a^{n-1} \equiv 1 \pmod n$ for all integers a with $\gcd(a, n) = 1$.

Uday
IT-21021

Step 1 : check 561 is composite square free

$$561 = 3 \times 11 \times 17$$

All factors are prime and distinct ⇒ square free

Step 2: Korselt's criterion:

A composite number n is a carmichael.

* n is square free.
* for every prime factor p, $p-1$ divides $n-1$

check

$n - 1 = 560$

$3 - 1 = 2$; $2 | 560$

$11 - 1 = 10$; $10 | 560$

$17 - 1 = 16$; $16 | 560$

So, 561 is a carmichael number.

Also Fermat test : a coprime to 561; $a = 2$

$$2^{560} \equiv 1 \pmod{561}.$$

95

Z_{17} is the group modulo of units mod 17.

order : $\phi(17) = 16$

possible orders must divide 16

Test $g = 3$:

$3^1 = 3, 3^2 = 9, 3^4 = 81 \equiv 13 = 13^2 \equiv 13^2 = 169 \equiv 16 \equiv$ mod

check

$3^8 \neq 1$, but $3^{16} \equiv 1$.

So 3 is a primtive root. mod 17.

Uday Talukder
IT-21021

Q6

Find x such that $3^x \equiv 13 \mod 17$

$3^1 = 3$

$3^2 = 9$

$3^3 = 27 \equiv 10$

$3^4 = 30 \equiv 13$

$x = 4$

Q7

Diffie-Hellman key Exchang:

*Relies on the hardness of the discrete log problem

* Two parties agree on a large prime panda generator g.

* Alice picks secret a, sends $g^a \mod p$.

* Bob picks secret b, sends $g^b \mod p$.

Uday
17-2(021

* Both compute shared key!

* · Alice : $(g^b)^a = g^{ab}$
  · Bob : $(g^a)^b = g^{ab}$

Without knowing a or b an attacker must solve the discrete log. problem.

Q8

Feature	substitution	Transpontion	play fair
Mechanism	Replaces each symbol with another	Rearranges position of symbol	Bigram substitution (digraphs)
Key space	Large (26! for mono-alphabetic	Dependson permutation Length	Based on 5x5 ke square
Freq. eney analysis	Weak - letter frequencies preserved	preserves letter freq not bigram. freq	obscures single letter freq bette
Example Plaintext	"Hellow"		

Uday
IT-21021

[Q5]

Given that,

$$E(x) = (5x + 8) \bmod 26$$

a) Encrypt "Dept of ICT MBSTU"

Step 1: We A=0, B=1, ... Z=25

Plain text (Spaces ignored for simplicity)

Dept of ICT MBSTU

letter → Numbers:

D=3, E=4, P=15, T=19 =O=14, F=5, I=8,

C=2, T=19, M=12, B=1, S=18, T=19, U=20

Encrypt each:

D	3	$(5\times3+8) = 23$ X
E	4	$(5\times4+8) = 28 \equiv 2$ C
P	15	$(5\times15+8) = 83 \equiv 5$ F
T	19	$(5\times19+8) = 103 \equiv 25$ Z

G	14	$(5\times14+8)=78\equiv0$	A
F	5	$(5\times5+8)=33\equiv7$	H
I	8	$(5\times8+8)=48\equiv22$	W
C	21	$(5\times2+8)=18$	S
T	19	$(5\times19+8)=25$	Z
M	12	$(5\times12+8)=68\equiv16$	Q
B	1	$(5\times1+8)=13$	N
S	18	$(5\times18+8)=98\equiv20$	U
T		25	Z
U	20	$(5\times20+8)=108=4$	E

ciphertext: XCFZAHWSZQNUZE

Uday
17-7-2021

B) Drive Decryption

Decrypt:

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

Need a^{-1} for $a = 5 \bmod 26$

possible value:

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

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

So,

$$D(y) = 21(y-8) \bmod 26.$$

Check decryption

Chipher $\cdot x = 23$

$D(23) = 21(23-8) = 21 \times 15 = 315 \equiv 3$ D

Vdoy
IT-2[illegible].21

§10

Step 1

Substitute : Shift each letter by key k_1.

Step 2:

Permute: Divide text into blocks and shuffle position inside each block using key k2.

Encryption process:

1. choose $K_1 = 3$ (shift)
2. Divide into blocks of size 4.
3. Permute each blocks with pattern.

E.g. [2, 4, 1, 3] Means 1st letter goes to position 2 [illegible]

Uday
IT-21021

Decryption process:

1. Reverse permutation for each block
2. Reverse shift by -3

cryptanalysis

Weakness

* If block size is small, frequency patterns remain
* only simple caesar shift => Vulnerable to frequency attack

Fixed permutation can be guessed.

Improvement:

- Use random PRNG for permutation
- Use a larger shift key space or polyalphabetic shift.