Unit 3

UNIT III **ASYMMETRIC CRYPTOGRAPHY** **9**

MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing – Factorization – Euler's totient function, Fermat's and Euler's Theorem – Chinese Remainder Theorem – Exponentiation and logarithm

ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange -– Elliptic curve arithmetic – Elliptic curve cryptography.

Fermat's Theorem

If p is prime and a is a positive integer not divisible by p, then ②

① $a^{p-1} \equiv 1 \pmod{p}$

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

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

$p \to 3$
$a \to 4$

$4^{3-1} \bmod 3 \Rightarrow 1$

$= 4^{2} \bmod 3$

$= 16 \bmod 3 \Rightarrow 1$ //

$p \to 3 \quad a \to 4$

$= 4^{3} \bmod p$

$= 64 \bmod 3$

$= \cancel{\frac{64}{3}}\ 21 \Rightarrow 1$ //

$4 \bmod 3 = 1$ //

Proof of Fermat's Theorem : To Prove $a^{p-1} \equiv 1 \pmod p$

1	Consider positive integers less than p	$P: \{1, 2, 3, \dots, p-1\}$
2	Multiply each element by a mod p	$X: \{a \bmod p, 2a \bmod p, \dots, (p-1)a \bmod p\}$
3	=> None of the elements is zero as 'a' is not divisible by p	
	=> None of the two elements are equal	Assume $ja \equiv ka \bmod p \quad 1 \le j < k \le p-1$ a is relatively prime to p $j \equiv k \bmod p$ (or) $\underline{j \bmod p} = \underline{k \bmod p}$ $\Rightarrow$ Impossible
	Multiplying all elements and taking mod p	

$$(1 \times 2 \times 3 \times \dots (p-1)) \bmod p \equiv \{a \times 2a \times 3a \times \dots \times (p-1)a\}$$

$$\cancel{(p-1)!} \bmod p \equiv a^{p-1} \times \cancel{(p-1)!} \Rightarrow 1 \bmod p \equiv a^{p-1}$$

Thank You

Euler's Totient Function $\phi(n)$

↳ phi

$\underline{4} \rightarrow 3, 2, 1$

$\gcd(x_i, 4) = 1$

the number of positive integers less than n and relatively prime to n.

$\phi(4) \Rightarrow 1, 2, 3 \Rightarrow 2$

$\gcd(1, 4) = 1$ ✓

$\gcd(2, 4) = 2$ ✗

$\gcd(3, 4) = 1$ ✓

① $\phi(\text{prime}) = \text{prime} - 1$

eg

$\phi(5) = 5 - 1 = 4$

$\phi(13) = 13 - 1 = 12$

② $\phi(1) = 1$

$\phi(8) = 1, 2, 3, 4, 5, 6, 7$

$GCD(1, 8) = 1$ ✓

$GCD(2, 8) = 2$

$G(3, 8) = 1$ ✓

$G(4, 8) = 4$

$G(5, 8) = 1$ ✓

$G(6, 8) = 2$

$G(7, 8) = 1$ ✓

$\phi(8) = 4$

Determine $\phi(37)$ and $\phi(35)$.

Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37. Thus $\phi(37) = 36$.

To determine $\phi(35)$, we list all of the positive integers less than 35 that are relatively prime to it:

$$1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18$$
$$19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34$$

There are 24 numbers on the list, so $\phi(35) = 24$.

More Examples

Table 2.6 Some Values of Euler's Totient Function $\phi(n)$

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

n	$\phi(n)$
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

n	$\phi(n)$
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

Theorem: If ‘p’ and ‘q’ are two prime numbers, n =pq then,

$$\phi(n) = \phi(pq) = \phi(p) \times \phi(q) = (p - 1) \times (q - 1)$$

Consider the set of positive integers less than n.	$\{1, 2, 3, \ldots, pq-1\}$
Integers in this set that are not relatively prime to n. Reason=> any integer that divides n must divide either of the prime numbers p or q. Therefore, any integer that does not contain either p or q as a factor is relatively prime to n.	$\{p, 2p, 3p, \ldots, (q-1)p\} \Rightarrow q-1$ $\{q, 2q, 3q, \ldots, (p-1)q\} \Rightarrow p-1$
The above two sets are non-overlapping. Hence total number of unique integers in the two sets which are not co-prime to n	$q-1+p-1 \Rightarrow q+p-2$
Total number of numbers co-prime to n are	$\phi(n) = n - (q+p-2)$ $= pq - q - p + 2$ $= (p-1)(q-1)$ //

Thank You

Eulers Theorem

Euler's theorem states that for every *a* and *n* that are relatively prime:

$$a^{\phi(n)} \equiv 1(\text{mod } n)$$

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

1. $a=3 \quad n=5$

$= 3^{\phi(5)} \bmod 5$

$= 3^{4} \bmod 5$

$= 81 \bmod 5 = 1$ //

2. $a=2 \quad n=3$

$= 2^{\phi(3)} \bmod 3$

$= 2^{2} \bmod 3$

$= 4 \bmod 3 = 1$ //

Proof:

$$a^{\phi(n)} \equiv 1(\mathrm{mod}\ n)$$

When n is prime $\Rightarrow$ Fermat's	$a^{\phi(p)} \equiv 1 \bmod p \Rightarrow a^{p-1} \equiv 1 \bmod p$
Consider the set of such integers that are relatively prime to n	$R = \{x_1, x_2, \ldots x_{\phi(n)}\}$
Multiply each element by a, modulo n	$S = \{ax_1 \bmod n, ax_2 \bmod n, \ldots, ax_{\phi(n)} \bmod n\}$

The above set is permutation of R because:
1. Because a is relatively prime to n and x_i is relatively prime to n, ax_i must also be relatively prime to n. Thus, all the members of S are integers that are less than n and that are relatively prime to n.
2. There are no duplicates in S.

LHS - S RHS - R

$$\prod_{i=1}^{\phi(n)} (ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod n$$

$$a^{\phi(n)} \times \left[\cancel{\prod_{i=1}^{\phi(n)} x_i}\right] \equiv \cancel{\prod_{i=1}^{\phi(n)} x_i} \pmod n$$

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

$ax_1 \bmod n \times ax_2 \bmod n \times \ldots ax_{\phi(n)} \bmod n$

Thank You

What is Prime Number?

1. **Prime numbers are numbers greater than 1 that only have two factors, 1 and the number itself.**
2. This means that a prime number is only divisible by 1 and itself.
3. If you divide a prime number by a number other than 1 and itself, you will get a non-zero remainder.
4. Any integer greater than 1 can be expressed as a product of prime factors:

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t}$$

$$\boxed{\begin{aligned} 91 &= 7 \times 13 \\ 3600 &= 2^4 \times 3^2 \times 5^2 \\ 11011 &= 7 \times 11^2 \times 13 \end{aligned}}$$

Primality Testing

Thank You