

Lecture Material#5

Information Security

Dr. Abu Nowshed Chy

Department of Computer Science and Engineering

University of Chittagong

nowshed@cu.ac.bd 01764207358

[Faculty Profile](#)



Modular Arithmetic

$$13^{13} \bmod 143 = 52$$





Fermat's Little Theorem

To compute $5^{301} \bmod 11$ using Fermat's Little Theorem, follow these steps:

Step 1: Recall Fermat's Little Theorem

Fermat's Little Theorem states:

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

where p is a prime number and $\gcd(a, p) = 1$.

Here, $a = 5$ and $p = 11$. Since $\gcd(5, 11) = 1$, Fermat's theorem applies:

$$5^{10} \equiv 1 \pmod{11}.$$



Fermat's Little Theorem

Step 2: Simplify $5^{301} \pmod{11}$

Write 301 in terms of multiples of 10 (the exponent from Fermat's theorem):

$$301 = 10 \times 30 + 1.$$

Thus:

$$5^{301} = (5^{10})^{30} \cdot 5^1.$$

Using Fermat's theorem, $5^{10} \equiv 1 \pmod{11}$, so:

$$(5^{10})^{30} \equiv 1^{30} \equiv 1 \pmod{11}.$$

Therefore:

$$5^{301} \equiv 1 \cdot 5^1 \pmod{11}.$$





Fermat's Little Theorem

Step 3: Compute $5^1 \pmod{11}$

$$5^1 = 5.$$

Final Answer:

$$5^{301} \equiv 5 \pmod{11}.$$

The result is 5.





Fermat's Little Theorem

1. Find $3^{31} \bmod 7$.

[Solution: $3^{31} \equiv 3 \bmod 7$]

By Fermat's Little Theorem, $3^6 \equiv 1 \bmod 7$. Thus, $3^{31} \equiv 3^1 \equiv 3 \bmod 7$.

2. Find $2^{35} \bmod 7$.

[Solution: $2^{35} \equiv 4 \bmod 7$]

By Fermat's Little Theorem, $2^6 \equiv 1 \bmod 7$. Thus $2^{35} \equiv 2^5 \equiv 32 \equiv 4 \bmod 7$.

3. Find $128^{129} \bmod 17$.

[Solution: $128^{129} \equiv 9 \bmod 17$]

By Fermat's Little Theorem, $128^{16} \equiv 9^{16} \equiv 1 \bmod 17$. Thus, $128^{129} \equiv 9^1 \equiv 9 \bmod 17$.





Euler's Theorem

Use Euler's theorem to find a number a between 0 and 99 such that a is congruent to 7^{402} modulo 1000.

Step 1: Recall Euler's theorem

Euler's theorem states:

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

where $\phi(n)$ is Euler's totient function and a and n are coprime.

Here, $a = 7$ and $n = 1000$. Since $\gcd(7, 1000) = 1$, Euler's theorem applies.





Euler's Theorem

Step 2: Calculate $\phi(1000)$

The prime factorization of 1000 is $1000 = 2^3 \cdot 5^3$. The totient function is:

$$\phi(1000) = 1000 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400.$$

Thus, $\phi(1000) = 400$.

Step 3: Apply Euler's theorem

By Euler's theorem:

$$7^{400} \equiv 1 \pmod{1000}.$$





Euler's Theorem

Step 4: Simplify $7^{402} \bmod 1000$

Write 402 as $400 + 2$:

$$7^{402} = 7^{400} \cdot 7^2.$$

Using Euler's theorem, $7^{400} \equiv 1 \pmod{1000}$. Thus:

$$7^{402} \equiv 1 \cdot 7^2 \pmod{1000}.$$

Step 5: Calculate $7^2 \bmod 1000$

$$7^2 = 49.$$





Euler's Theorem

Final Answer:

$$7^{402} \equiv 49 \pmod{1000}.$$

The number a is 49.

Use Euler's theorem to find a number a between 0 and 99 such that a is congruent to 7^{402} modulo 13.





RSA Algorithm Steps

<https://www.chiragbhalodia.com/2021/09/rsa-algorithm-with-example.html>

RSA Algorithm Steps

Step-1: Select two prime numbers p and q where $p \neq q$.

Step-2: Calculate $n = p * q$.

Step-3: Calculate $\Phi(n) = (p-1) * (q-1)$.

Step-4: Select e such that, e is relatively prime to $\Phi(n)$, i.e. $(e, \Phi(n)) = 1$ and $1 < e < \Phi(n)$

Step-5: Calculate $d = e^{-1} \bmod \Phi(n)$ or $ed = 1 \bmod \Phi(n)$.

Step-6: Public key = $\{e, n\}$, private key = $\{d, n\}$.

Step-7: Find out cipher text using the formula,

$C = P^e \bmod n$ where, $P < n$ where C = Cipher text, P = Plain text, e = Encryption key and n =block size.

Step-8: $P = C^d \bmod n$. Plain text P can be obtain using the given formula. where, d = decryption key





RSA Algorithm Steps

Step – 1: Select two prime numbers p and q where $p \neq q$.

Example, Two prime numbers $p = 13$, $q = 11$.

Step – 2: Calculate $n = p * q$.

Example, $n = p * q = 13 * 11 = 143$.

Step – 3: Calculate $\Phi(n) = (p-1) * (q-1)$.

Example, $\Phi(n) = (13 - 1) * (11 - 1) = 12 * 10 = 120$.

Step – 4: Select e such that, e is relatively prime to $\Phi(n)$, i.e. $(e, \Phi(n)) = 1$ and $1 < e < \Phi(n)$.

Example, Select $e = 13$, $\gcd(13, 120) = 1$.





RSA Algorithm Steps

Step – 5: Calculate $d = e^{-1} \bmod \Phi(n)$ or $e * d = 1 \bmod \Phi(n)$

Example, Finding d: $e * d \bmod \Phi(n) = 1$

$$13 * d \bmod 120 = 1$$

(How to find: $d * e = 1 \bmod \Phi(n)$)

$$d = ((\Phi(n) * i) + 1) / e$$

$$d = (120 + 1) / 13 = 9.30 (\because i = 1)$$

$$d = (240 + 1) / 13 = 18.53 (\because i = 2)$$

$$d = (360 + 1) / 13 = 27.76 (\because i = 3)$$

$$d = (480 + 1) / 13 = 37 (\because i = 4)$$

Step – 6: Public key = $\{e, n\}$, private key = $\{d, n\}$.

Example, Public key = $\{13, 143\}$ and private key = $\{37, 143\}$.





RSA Algorithm Steps

Step – 6: Public key = $\{e, n\}$, private key = $\{d, n\}$.

Example, Public key = $\{13, 143\}$ and private key = $\{37, 143\}$.

Step – 7: Find out *cipher text* using the formula, $C = P^e \bmod n$ where, $P < n$.

Example, Plain text $P = 13$. (Where, $P < n$)

$$C = P^e \bmod n = 13^{13} \bmod 143 = 52.$$

Step – 8: $P = C^d \bmod n$. Plain text P can be obtain using the given formula.

Example, Cipher text $C = 52$

$$P = C^d \bmod n = 52^{37} \bmod 143 = 13.$$





RSA Algorithm

P and Q are two prime numbers. $P=7$ and $Q=17$. Take a public key $E=5$, generate the private key.





RSA Algorithm

P and Q are two prime numbers. $P=7$, and $Q=17$. Take public key $E=5$. If plain text value is 6, then what will be cipher text value according to RSA algorithm? Again calculate plain text value from cipher text.

In a public key cryptosystem using RSA algorithm, user uses two prime numbers 5 and 7. He chooses 11 as Encryption key, find out decryption key. What will be the cipher text, if the plaintext is 2? Decrypt the cipher text, what will be the value of plain text?

P and Q are two prime numbers. $P=17$, and $Q=11$. Take public key $E=7$. If plain text value is 5, then what will be cipher text value & private key value according to RSA algorithm? Again calculate plain text value from cipher text.





RSA Algorithm



Practice Materials

<https://www.chiragbhalodia.com/2021/09/rsa-algorithm-with-example.html>

