Notes 10/26/23

James Meegan

November 2, 2023

Public Key Cryptography

Alice and Bob need to communicate without using a secret preshared key.

Pass Protocol

3 pass protocol gives a way to do this securely. Sending everything 3 times is inefficient and it is vulnerable to a man in the middle attack.

Man in the middle attack

Eve pretends to be Alice to Bob and pretends to be Bob to Alice and captures their message during the passing.

Three-Pass Protocol in Cryptography

The three-pass protocol allows two parties, Alice and Bob, to exchange a message without either party having to reveal their secret keys to the other. This is done in three passes, hence the name.

1. Alice sends Bob a transformed version of her message.
2. Bob transforms the received message and sends it back to Alice.
3. Alice performs the final transformation and retrieves Bob's message.

Tools for Modular Exponents with Composite Numbers

We need tools to work with exponents modulo composite numbers.

Euler's Theorem

If $\gcd(a, m) = 1$, then

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

where $\phi(m)$ counts how many residues (mod m) have an inverse.

Example:

$$3^{\phi(20)} \equiv 1 \pmod{20}$$

Given:

$$a = 3 \pmod{20}$$

$$\gcd(3, 20) = 1$$

To find:

$$\phi(20)$$

We use:

$$\phi(20) = \phi(4) \cdot \phi(5)$$

$$\phi(4) = 2(2 - 1) = 2$$

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

Thus, $\phi(20) = 2 \times 4 = 8$.

Let p be prime:

$$\phi(p^k) = p^k(1 - \frac{1}{p})$$

$$\Rightarrow \phi(p) = p(1 - \frac{1}{p}) = p(p - 1)$$

Check using Repeated Squaring

$$\begin{aligned} 3^2 &\equiv 9 \pmod{20} \\ 3^4 &= (3^2)^2 \equiv 81 \equiv 1 \pmod{20} \\ 3^8 &= (3^4)^2 \equiv 1 \pmod{20} \end{aligned}$$

Example for $6 \pmod{20}$

Note: Euler's theorem doesn't work in this case.

Given:

$$\begin{aligned} a &= 6 \\ m &= 20 \\ \gcd(20, 6) &= 2 \neq 1 \end{aligned}$$

Calculate:

$$\begin{aligned}
6^2 &\equiv 36 \equiv 16 \pmod{20} \\
6^4 &= (6^2)^2 = 256 \equiv 16 \pmod{20} \\
6^8 &= 16^2 \equiv 256 \equiv 16 \pmod{20}
\end{aligned}$$

Example for $5^{37} \pmod{21}$

Note: 21 is not prime.

Using Euler's theorem where $\gcd(5, 21) = 1$,

$$\begin{aligned}
\phi(21) &= \phi(3) \times \phi(7) \\
&= (3-1)(7-1) \\
&= 2 \times 6 = 12
\end{aligned}$$

$$\begin{aligned}
5^{36} &= (5^{12})^3 \equiv 1 \pmod{21} \\
5^{37} &\equiv 5^{36+1} = 5^{36} \times 5^1 \equiv 5 \pmod{21}
\end{aligned}$$

General Rule for Exponents modulo Composite m

If your equation is $\pmod{m}$,
all of the exponents modulo $\phi(m)$
You have to be careful if the base and modulus have any shared factors.

Example for $7^{13} \pmod{10}$

$$\begin{aligned}
\phi(10) &= \phi(2) \times \phi(5) \\
&= (2-1)(5-1) \\
&= 4
\end{aligned}$$

$$\begin{aligned}
13 &\equiv 1 \pmod{4} \\
7^{13} &= 7^1 \equiv 7 \pmod{10} \\
7^{14} &= 7^2 = 49 \equiv 9 \pmod{10} \\
14 &\equiv 2 \pmod{4}
\end{aligned}$$

RSA

Rivest, Shamir, Adleman discovered RSA in the 1970s.

Public Key Cryptosystem

Alice creates a public key that she can tell everyone.

Anyone can encrypt a message using this key.

Alice is the only one who can decrypt messages.

Alice picks two large secret prime numbers p and q, for example, 10^{20}.

She computes $n = p \times q$.

She picks an encryption exponent e such that

$$\gcd(e, (p-1)(q-1)) = 1$$

In practice, $e \approx 65537$.

Alice's public key is (n, e).

Anyone can send Alice a message m using the encryption function

$$E(x) \equiv x^e \pmod{n}$$

Alice wants to decrypt:

$$D(y) = y^d \pmod{n}$$

We have:

$$M = D(M^e)$$

$$M = D(M^e) \equiv (M^e)^d \equiv M^{ed} \pmod{n}$$

So,

$$d \equiv e^{-1} \pmod{\phi(n)}$$

Alice can use p and q to find

$$\phi(n) = \phi(p) \times \phi(q)$$

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

She computes:

$$d = e^{-1} \pmod{(p-1)(q-1)}$$

Where d is Alice's secret private key. She can forget p and q.