week 2
Part 3

RSA

Difference between Diffie-Hellman and RSA?

Diffie-Hellman is mainly used for key exchange in asymmetric cryptography. for symmetric encryption we need a secret key or a symmetric key that both the sender and the receiver can use and how we exchange that key secretly is the main idea of Diffie-Hellman. RSA is strictly asymmetric cryptography. By asymmetric we know that it has the concept of Private, Public key pair. RSA enables us to understand the difference between encryption and digital signature. we can use it for both encryption or digital signature.

RSA example,

At first we need to choose two large prime numbers P and Q let's say P=3 and Q=5. Now, we need to Compute P×Q and (P-1)×(Q-1),

$$P \times Q = 3 \times 5 = 15$$
$$(P-1) \times (Q-1) = (3-1) \times (5-1) = 2 \times 4 = 8$$

Next, we need to ~~find~~ Select a value that is relatively Prime to 8. By relatively prime, it means they do not have any common factor except 1. Let's say e=3 as 3 and 8 do not have any common factor. Next, we need to find another value d. Here, we need to use a formula; (d*e)% 8 and it should be equal to 1. Basically, (d×3)% 8 = 1 we need to select such a value for d so, that the answer is 1. we can say d=11 for this example.

So, the Public Private key pair looks like,

Public key $(e, 15) = (3, 15)$ [15 is from P*Q]

Private key $(d, 15) = (11, 15)$

Let's assume that our plain text is 2 and finally we need to show the calculation behind encryption and decryption.

For encryption we need to apply the formula,

$$\begin{aligned} \text{Ciphertext} &= 2^e \bmod 15 \\ &= 2^3 \bmod 15 \\ &= 8 \end{aligned}$$

For decryption we need to apply similar formula but use d instead and Ciphertext.

$$\begin{aligned} \text{Plaintext} &= 8^d \bmod 15 \\ &= 8^{11} \bmod 15 \\ &= 2 \end{aligned}$$

RSA in Practice

Why do RSA works?

It works because although having knowledge of the Public key, it doesn't reveal the Private key.

Both the Public and private keys contain the important number n and n is basically the product of two large Prime numbers p and q. The security of the system relies on that n is hard to factor. By the word "factor" or "factorization" is that, if we have a large number even the one which has only 2 Prime factors, there is no easy way to discover what they are. The whole RSA depends on factorization.

Is it Possible to break RSA with a brute for?

Yes, it is possible by simply factorising n, to make this difficult, its recomended that p and q be chosen so that n is at least 1024 bits.

One excellent feature of RSA is that it is Symmetrical because we can use the Public key then private key or use Private key then Public key for decryption.

Disadvantage of RSA,

RSA algorithm operates with huge numbers, and involves lots of exponentiation, repeated multiplication and modulus. Such operations are computationally expensive and so, RSA encryption and decryption are incredibly slow, even on fast computers.