Page :
Date : / /

ASSIGNMENT B3

Title : Diffie-Hellman Key Exchange

Problem Statement : Implementation of Diffie-Hellman Key Exchange

Objective :

1. To understand how Diffie-Hellman key exchange algorithm works
2. Implementation of Diffie-Hellman key exchange

Outcome : Succesfully implemented and understood Diffie-Hellman key exchange algorithm.

Requirements : python3, jupyter, mpmath

Concepts Related Theory

- Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curve over finite fields. ECC requires a smaller key as compared to non-ECC cryptography to provide equivalent security (a 256-bit ECC security has security equivalent to 3072-bit RSA)

- An elliptic curve is a planar algebraic curve defined by: $y^2 = x^3 + ax + b$, where a is the coefficient of x and b is the constant of the equation. The curve is non-singular, i.e, its graph has no cusps or self-intersections (when the characteristic of the coefficient field is equal to 2 or 3).

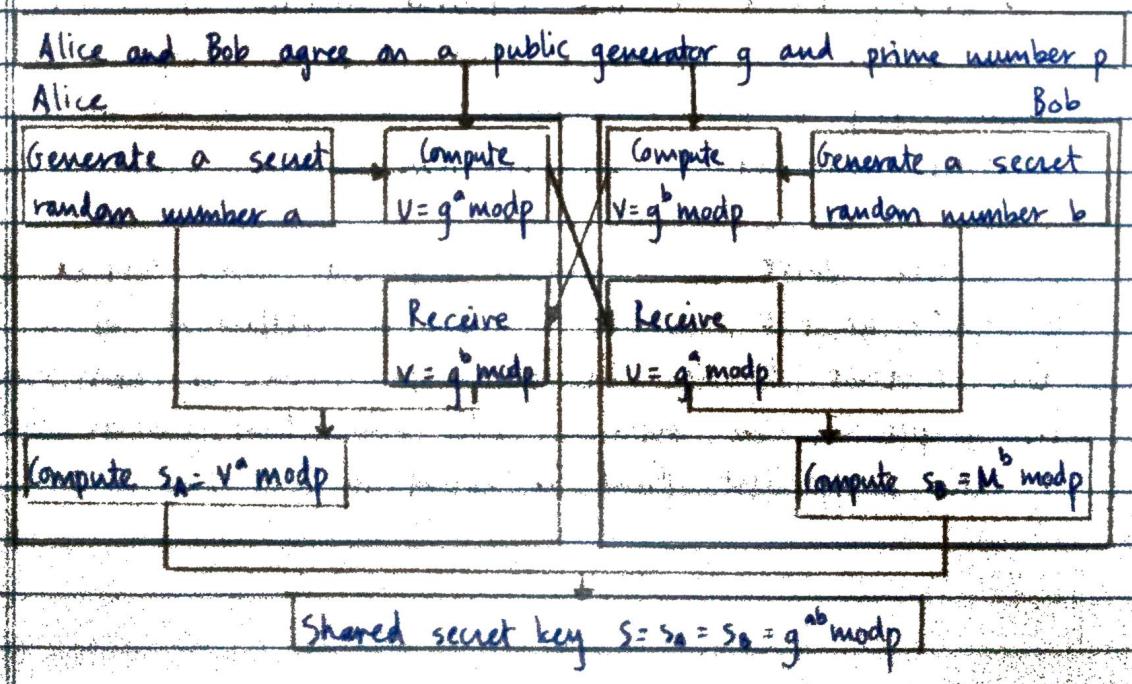
Page :
Date : / /

The Diffie-Hellman algorithm is used to establish a certain shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

Diffie-Hellman (DH) is a simple public-key exchange algorithm for securely exchanging cryptographic keys over a public communication channel. Keys are not actually exchanged - they are jointly derived. It is named after their inventors Whitfield Diffie and Martin Hillman. Note that the public key encryption schemes are only secure if authenticity of public key is assured.

The protocol enables 2 users to establish a secret key using a public key based scheme using discrete algorithms. The protocol is secure only if the authenticity of the participants can be established.

Algorithm:



Page :
Date : / /

Test Cases

Test Case	Expected Output	Actual Output
Modulus chosen : 95	A's calculated value	A's secret key
Base chosen : 23	49	64
Number chosen by A : 330	B's calculated value	B's secret key
Number chosen by B : 905	93	64

Conclusion :

Succesfully understood and implemented Diffie-Hellman key exchange algorithm