Honours Assignment - 2

Abras Kaleem
SSR
12

1. Write an algorithm for generating public and private key using elliptical curve cryptography.

Ans. * Choose a prime number p and an elliptic curve $y^2 = x^3 + ax + b \pmod p$.

* Choose a point G on the curve, called the generator point.
* Choose a private key d, a random integer between 1 and p-1.
* Calculate the corresponding public key $Q = d * G$
* Private key d is kept secret, while the public key Q is made public
* To generate the key pair, the following steps can be used:
  - → Generate a random prime number p. This will be the prime modulus for the curve.
  - → Choose the coefficients a and b for the elliptic curve equation $y^2 = x^3 + ax + b \pmod p$
  - → Choose a point G on the curve that will be the generator point. This point G on the curve that will be the generator point. This point should have a large prime order (a large number of points on the curve that can be multiplied by G to give another point on the curve).
  - → Generate a random private key d, a random integer between 1 and p-1
  - → Calculate the corresponding public key $Q = d * G$.
  - → This private key d is kept secret, while the public key Q is made public
  - → This algorithm can be used to generate a key pair for use with elliptic curve cryptography. The security of the key pair depends on the strength of the prime number p and the randomness of the private key d.

2. Is Diffie-Hellman ~~key~~ key exchange protocol vulnerable? Justify.

Ans. The Diffie-Hellman key exchange protocol is vulnerable to man-in-the-middle attacks. In a man-in-the-middle attack, an attacker can intercept the communication between the two parties who are trying to establish a shared secret and pretend to be each party to the other, effectively establishing separate ~~connections~~ connections with both parties. This allows the attacker to obtain the shared secret and decrypt the communication.

To protect against man-in-~~the~~ the-middle attacks, it is important to authenticate the ~~identities~~ identities of the parties involved in the Diffie-Hellman key exchange. This can be done through the use of digital certificates or by securely verifying the ~~identity~~ identities of the parties through some out-of-band method.

Additionally, the Diffie-Hellman key exchange is vulnerable to mathematical attacks if the parameters used (such as the prime modulus and generator) are not chosen properly. It is important to use strong parameters to ensure the security of the key exchange.

Overall, while the Diffie-Hellman key exchange protocol is a ~~so~~ secure method for establishing a shared secret over an insecure ~~com~~ communication channel, it is important to implement appropriate security ~~mea~~ measures to protect ~~again~~ against potential attacks.