# Name in the middle attacks in the exchange.

Name Description Advantages Disadvantages RSA Algorithm RSA is a cryptosystem which is known as one of the first practicable public-key cryptosystems and is widely used for secure data transmission 1. it is public key cipher 2. RSA algorithm is hard to crack. 3. RSA algorithamuses the public key to encrypt data. 1. Slow signing and decryption, which are slightly tricky to implement securely. 2.

Very slow key generation. 3. Key is vulnerable to various attacks if poorly implemented. Diffie Hellman A simple public-key algorithm is Diffie-Hellman key exchange . This protocol enables two users to establish a secret key using a public-key scheme based on discrete logarithms. 1. The sender and receiver have no prior knowledge of each other.

2. Communication can take place through an insecure channel. 3. Sharing of secret key is safe. 1. can not be used for symmetric key exchange.

2. can not used for signing digital signatures. 3. the nature of diffie-hellman key exchange does make it susceptible to man in the middle attacks in the exchange.

Digital Signature DSS is uses the secure hash algorithm a digital signature is an authentication mechanism that enable the creator of a message to attach a code that acts as a signature. 1. Non repudiation, because the author cannot be denied of his work(he created and sent).

2. Imposter prevention Integrity of data, ever change will be detected.

1.

Expiry: Digital signatures, like all technological products, are highly dependent on the technology it is based on. Hash Function Hash function also called as message digest and one way encryption, are in some sense use no key. 1. the  main advantage is syncronization. 2. in many situations, hash tables turn out more efficient than lookup structures. 1.

hash collisions are practically unavoidable. 2. hash tables becomes quite inefficient when there are many collisions.