**Chapter 7: PKI and Cryptographic Applications**

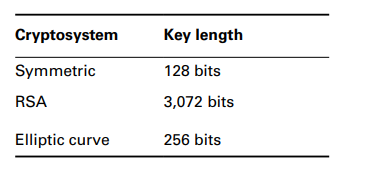
RSA is the most popular public key cryptography algorithm. The RSA algorithm depends on the computational difficulty inherent in factoring the product of large prime numbers. Keys must be chosen sufficiently large as compared to the symmetric key algorithm to protect against cryptanalysis attacks.

The Diffie–Hellman key exchange algorithm uses large integers and modular arithmetic to facilitate the secure exchange of secret keys over insecure communications channels. This is known as the discrete logarithmic problem.

ElGamal - ElGamal extended Diffie–Hellman key exchange algorithm to support an entire public key cryptosystem used for encrypting and decrypting messages. Major disadvantage was that ElGamal doubles the size of the message that it encrypts.

Elliptic Curve - It is based on the elliptic curve discrete logarithm problem. It is widely believed that this problem is harder to solve than both the prime factorization problem that the RSA cryptosystem is based on and the standard discrete logarithm problem utilized by Diffie–Hellman and ElGamal.

The three cryptosystems provide the same level of protection with different key size.



Quantum computing is an area of advanced theoretical research in computer science and

physics. The theory behind them is that we can use principles of quantum mechanics to

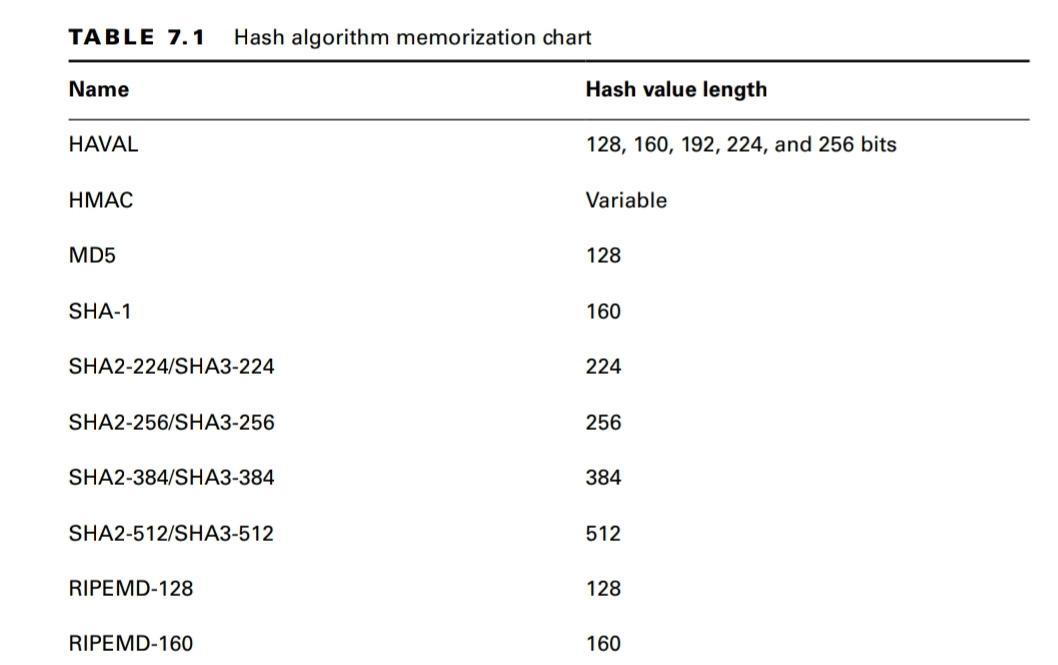
replace the binary 1 and 0 bits of digital computing with multidimensional quantum bits known as qubits.

Hash function takes input of any size and produces a fixed length output called message digest.

MD5, SHA1 and RIPEMD-128 are not considered secure anymore.

SHA3 provides the same level of security as SHA2 but is relatively slower. Therefore, it is not used commonly. Military and federal government uses it.

SHA2 is secure and comes in four variants - SHA-256, SHA-512, SHA-224(**256-32**), SHA-384(**512-128**)



Digital Signature - Sender computes the message digest for the plaintext message. The digest is then encrypted with the sender's private key. This encrypted message digest is called the digital signature. The digital signature is then appended to the plaintext message and the entire message is encrypted with the receiver's public key.

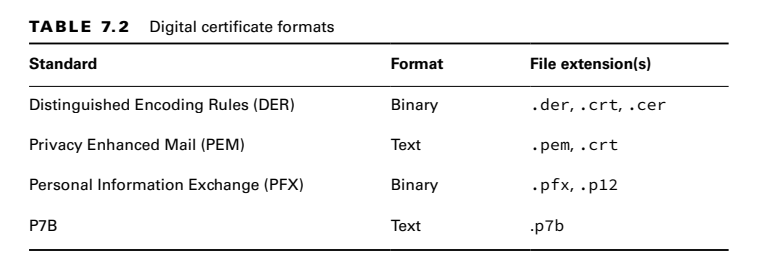
It is to be noted that digital signatures only provide authentication, non-repudiation, and integrity. Confidentiality is achieved using an extra step utilizing the receiver's public key.

HMAC implements partial digital signature, it provides integrity but does not provide non-repudiation. Instead of computationally expensive digital signatures, it uses a shared secret key for encrypting message digest.

Digital Signature Standard - NIST specifies all federally approved digital signature algorithms in this document which are

* SHA-3 hashing functions
* DSA (soon going to be replaced with Edwards-curve DSA)
* RSA
* ECDSA

Digital certificates are endorsed copies of an individual’s public key. When users verify that a certificate was signed by a trusted certificate authority (CA), they know that the public key is legitimate. Their construction is governed by an international standard —X.509.



Certificate Authorities are the neutral organizations that offer notarization services for digital certificates. To obtain a digital certificate from a reputable CA, you must prove your identity to the satisfaction of the CA.

In the CA trust model, the use of a series of intermediate CAs is known as certificate

chaining. Root CA (offline) issues certificates for intermediate CA's (online) which issues certificates to end users. The trust is traced back up to the root CA while validating the certificate.

Once you’ve satisfied the certificate authority regarding your identity, you provide them

with your public key in the form of a certificate signing request (CSR).

You can check if the certificate was revoked using a certificate revocation list (CRL) or the Online Certificate Status Protocol (OCSP).

PGP secure email system combines the CA hierarchy concept with the “web of trust”. It provides email message security using digital signatures and public key encryption.

**TLS Cipher suite example -** TLS\_DH\_RSA\_WITH\_AES\_256\_CBC\_SHA384

DH is key exchange algorithm, RSA is public key algorithm used to prove server identity (authentication), AES is bulk encryption algorithm, and SHA 384 is hashing algorithm to create message digest.

Circuit Encryption

* Link encryption protects entire communications circuits by creating a secure tunnel between two points (link). It encrypts complete packets including headers when entering the tunnel. For the packet to travel across multiple hops, it needs to be re-encrypted for each link increasing the routing complexity.
* End-to-end encryption protects communications between two parties (for example, a client and a server) and is performed independently of link encryption.

**Cryptographic attacks**

* Known plaintext and chosen plaintext attacks require the ability to encrypt data.
* Fault injection attacks require physical access to the facility.
* Birthday attack is based on the birthday paradox and tries to find collisions in hashing algorithms.
* Meet-in-the-middle attack is used to defeat encryption algorithms that use two rounds of encryption like 2DES.