Assumptions

Encryption

A1. Symmetric key cryptography is also called conventional or secret-key cryptography.

A2. Public key cryptography is also called asymmetric key cryptography.

A3. In symmetric key crypto, the same secret key, K, is used for encryption, E(), and decryption, D(). The secret is shared between two entities, i.e. K_{AB}.

A4. In public key crypto, there is a pair of keys, public (PU) and private (PR). One key from the pair is used for encryption, the other is used for decryption. Each entity has their own pair, e.g. (PU_A, PR_A).

A5. Encrypting plaintext (or a message), P or M, with a key, produces ciphertext C, e.g. $C = \mathrm{E}(K_{AB}, P)$ or $C = \mathrm{E}(PU_A, M)$.

A6. Decrypting ciphertext with the correct key will produce the original plaintext. The decrypter will be able to recognise that the plaintext is correct (and therefore the key is correct). E.g. $P = \mathrm{D}(K_{AB}, C)$ or $M = \mathrm{D}(PR_A, C)$.

A7. Decrypting ciphertext using the incorrect key will *not* produce the original plaintext. The decrypter will be able to recognise that the key is wrong, i.e. the decryption will produce unrecognisable output.

Knowledge of Attacker

A8. All algorithms used in cryptography, e.g. encryption/decryption algorithms, hash functions, are public.

A9. An attacker knows which algorithm is being used, and any public parameters of the algorithm.

A10. An attacker can intercept any message sent across a network.

A11. An attacker does not know secret values (e.g. symmetric secret key K_{AB} or private key PR_A).

A12. Brute force attacks requiring greater than 2^{80} operations are impossible.

Authentication with Symmetric Key and MACs

A13. An entity receiving ciphertext that successfully decrypts with symmetric secret key K_{AB} knows that the original message has not been modified and that it originated at one of the owners of the secret key (i.e. A or B).

A14. An entity receiving a message with attached MAC that successfully verifies, knows that the message has not been modified and originated at one of the owners of the MAC secret key.

Hash Functions

A15. A cryptographic hash function, H(), takes a variable sized input message, M, and produces a fixed size, small output hash, h, i.e. $h = \mathrm{H}(M)$.

A16. Given a hash value, h, it is impossible to find the original message M.

A17. Given a hash value, h, it is impossible to find another message M' that also has a hash value of h.

A18. It is impossible to find two messages, M and M', that have the same hash value.

Digital Signatures

A19. A digital signature of a message M is the hash of that message encrypted with the signers private key, i.e. $S = \mathrm{E}(PR, \mathrm{H}(M))$

A20. An entity receiving a message with an attached digital signature knows that that message originated by the signer of the message.

Key Management and Random Numbers

A21. A secret key can be exchanged between two entities without other entities learning its value.

A22. Any entity can obtain the correct public key of any other entity.

A23. Pseudo-random number generators (PRNG) can generate effectively true random numbers.

Principles

P1. *Experience*: Algorithms that have been used over a long period are less likely to have security flaws than newer algorithms.

P2. *Performance*: Symmetric key algorithms are significantly faster than public key algorithms.

P3. *Performance*: The time to complete a cryptographic operation is linearly proportional with the input data size.

P4. *Key Distribution*: Keys should be distributed using automatic means.

P5. *Key Re-use*: The more times a key is used, the greater the chance of an attacker discovering that key.

P6. *Multi-layer Security*: Using multiple overlapping security mechanisms can increase the security of a system.