Glossary

AEAD Authenticated Encryption with Additional Data. A modern mode of encryption that provides in-built authenticity, usually via the computation of a MAC that is computed over the message or ciphertext, and additional data that requires protection.

AES The Advanced Encryption Standard. The most commonly used block cipher. The Rijndael algorithm was developed by researchers in Belgium as a response to a NIST call for replacements for DES.

Asymmetric Encryption Encryption that uses two keys, one for encryption and one for decryption. Traditionally only one of the keys is kept private.

Block Cipher An encryption algorithm that operates on data of a fixed size - a block - and returns data of the same size.

Certificate Authority A company that is permitted to sign digital certificates. Which companies can do this is usually specified by those whose root certificates (containing the CA public key) are shipped with modern operating systems or browsers.

ChaCha20 A modern stream cipher, often paired with the Poly1305 MAC. Uses only basic CPU operations, and as such is extremely fast on modern devices, particularly phones. Used as standard on Android phones when connecting to Google servers. It is also an available cipher suite in TLS.

Cipher Block Chaining A mode of operation in which the output of a block n is XOR'd with the input to the next block n+1. This improves on ECB mode by ensuring identical messages encrypt to different things. The first block is XOR'd with an IV. This mode is sometimes used, but has some security vulnerabilities. It also cannot be parallelised, which makes it inefficient.

Ciphertext An encrypted message.

Confidentiality The prevention of unauthorised users from accessing some data.

Confusion The mapping between input and output of some process is hard to predict, usually because the output depends on multiple parts of the key.

Counter Mode A mode of operation in which a nonce+counter is encrypted, and that is XOR'd with the corresponding message block. Can be parallelised, and is very secure as long as the nonce is not reused. Nonce reuse means the same keystream is used twice, which is a big security vulnerability, and makes it possible to recover unencrypted message bits.

DES The Data Encryption Standard. A commonly used Feistel Cipher developed at IBM. It suffered from having an unusually short key length of 56 bits, due to interference from the NSA. It is now too easy to brute force the key.

Diffie-Hellman	The most common key exchange mechanism, and a protocol that underpins almost all modern secure communication. Relies on the difficulty of solving the discrete logarithm problem.
Diffusion	A single change in the input, will lead to multiple changes in the output. In a sense this is related to the idea of randomness; if the output is to appear random, about half should change for any change in the input.
Digital Certificate	A specific document (usually X.509 format) that contains a public key, and is signed by a certificate authority. By verifying the signature, we obtain a sense of trust in the public key contained within the certificate.
Digital Signature	A hash of a message or document that is encrypted by a private key. A receiver can verify this signature by using the sender's public key. This provides authentication of the identity of the sender.
DSA	Digital Signature Algorithm. A protocol used for digital signatures, the mathematics of which is similar to Diffie-Hellman, that is exponents and modular arithmetic. DSA is popular because it can also be improved through the use of elliptic curves, usually called ECDSA.
Electronic Codebook	A basic mode of operation in which each block of message is encrypted one after another, one block in, one ciphertext block out. Has a tendency to leak information about the data, even when encrypted. Use of this mode is strongly discouraged!
Elliptic Curves	Curves of the form $y^2 = x^3 + ax + b$. Used as a replacement for modular arithmetic in Diffie-Hellman and DSA. Perform a similar function to modular arithmetic, but require shorter keys to be as secure, and so are more efficient.
Ephemeral Mode	A new key exchange occurs at the beginning of each new session or communication, rather than long term use of shared secrets. Provides perfect forward secrecy.
Feistel Cipher	An alternative to an SP-Network for the development of block ciphers. Uses permutation function (e.g. a hash function) in a series of rounds that, through the design of the Feistel cipher, are then reversible. In other words, a Feistel cipher is a mechanism to turn any pseudorandom function, into a block cipher.
Galois Counter Mode	A modern mode of operation often seen used with AES. GCM is similar to counter mode, but also computes a message authentication code or GMAC over the data, ensuring message authenticity.
Handshake	A protocol that establishes the various security parameters required for secure communication, such as cipher suites and shared secrets.
Hash Function	A function that takes a message of any length, and returns a message of a fixed size. Used frequently in message authentication codes and digital signatures. Also sometimes used to secure passwords, and to derive keys from shared secrets like Diffie-Hellman output.

HMAC	An improved structure for a MAC, using two derived keys and two applications of a hash function. Solves an issue of length extension attacks on MACs used with SHA-1 or SHA-2.
Integrity	The prevention of unauthorised users from modifying some data.
IV	Initialisation Vector. A random string that is not secret, and used to provide randomness. Usually it is required that IVs may repeat (at random), but should be strongly random and as such, unpredictable.
Key	The secret component of most ciphers. A string of bytes that are used to alter the output of a cipher, such that it cannot be reversed without possessing those same bytes.
Key Exchange	A protocol that allows two parties to generate or share a secret key over an insecure channel.
Key Expansion	A function that takes a fixed length key and expands it into a series of bits for use between rounds of a block cipher. This is similar in operation to a stream cipher, but the key expansion is only required to function for a fixed length (depending on the algorithm), not indefinitely.
Key Mixing	Using XOR to combine a key into a message between rounds of encryption. It is this process that ensures a cipher cannot be reversed without the key.
MD5	A historic hash function with a block size of 128-bits. Sometimes usable as a checksum, but otherwise deemed unsecure now.
Message Authentication Code (MAC)	A tag appended to a message that provides authenticity. A shared secret is combined with the message and hashed, to provide a tag that is able to verify whether a message has been changed.
Message Authenticity	The knowledge that a message hasn't been altered, and that it has come from the correct sender. In this case, the correct sender is someone also in possession of the shared secret key.
Mode of Operation	A protocol within which a block cipher is used, in order to facilitate the encryption of messages of arbitrary lengths. Modern modes of operation often provide useful features beyond the core block cipher, such as message authentication.
Nonce	A "number used once". A string of bytes that are used once in combination with a key, to provide different permutations (e.g. a random keystream) as required. Most commonly seen when combined with stream ciphers, or block ciphers in a mode of operation such as counter mode.
One-time Pad	A perfectly secure encryption mechanism that uses a key the same length as the message. Each part of the key is XOR'd with the corresponding part of the plaintext

Padding	Additional bytes added to a message as required to bring the message to the required size of a block cipher or hash function.
Perfect forward secrecy	The compromise of a shared key does not allow an attacker to a also decrypt past messages. In other words, there is no one secret that allows many historic messages to be decrypted. Usually achieved by ephemeral diffie-hellman.
Permutation Box	A reversible process through which bits are moved and mixed to spread out changes through a block of data.
Plaintext	An unencrypted message.
Poly1305	A modern MAC that is often used with ChaCha20. It's name is derived from the polynomial functoin used within it, 2^130-5.
Public-key Cryptography	Another term that is commonly used to refer to asymmetric encryption, but also encompases key exchange mechanisms such as Diffie-Hellman.
Random Number	A cryptographicaly random number is a number which is statistically random, for as long as is required. Cryptographically secure random numbers are held to a much higher level of security than standard random numbers. Each operating system includes a function that obtains such numbers, usually incorporating hardware randomness to improve the output.
Round Function	Some repeated process within a cipher. Often found in ciphers and hash functions, rounds usually involve some permutation and substitution, and are repeated many times to ensure that the output is statistically random.
RSA	The most commonly used public-key cryptographic system. Provides a public and private key pair, either of which can be used for encryption, with the other reversing this process. RSA is used for encryption and for signing. RSA is based around the difficulty of solving the integer factorisation problem.
SHA-1	A hash function with a 160-bit block size. Still secure within structures like HMAC, but a collision has been found, so security advice is to move toward SHA-2 at this point.
SHA-2	Very similar to SHA-1, but with a 256 or 512-bit block size. This increased block size makes collisions much more difficult, and this function is currently considered secure.
SHA-3	An alternative to SHA-2, should a serious vulnerability with SHA-2 be found. Offers similar hash lengths, but the function itself is very different to SHA-1 and SHA-2.
SP-Network	An encyption structure that chains substitution and permutation operations one after another. This is commonly employed in block ciphers.
SSL	Secure Socket Layer. A handshake and transmission protocol for internet traffic. SSL is the historic name, of which there were numerous versions 1.0, 2.0 and 3.0.

Stream Cipher	An encryption algorithm that operates on data of any size, returning ciphertext of the same size. Traditionally generates a pseudorandom keystream, XORing each part of the key with the corresponding part of the plaintext.
Substitution Box	A reversible process through which bits or bytes are substituted with others in a fixed lookup table. In most cases these lookup tables are designed with the algorithm, rarely (e.g. the Blowfish block cipher) they are generated at runtime based on the key.
Symmetric Encryption	Encryption that uses a single key for both encryption and decryption.
TLS	Transport Layer Security. The modern equivalent of SSL, replacing it as of SSL 3, TLS 1. Current version is 1.2, with 1.3 in draft.
XOR	A binary operator on two inputs, with one output. "A OR B, but not A AND B"