Basic Cryptographic Methods / Definitions

* Confidentiality
  + Definition: The dictionary definition of confidentiality is, “the state of keeping or being kept secret of private.” Confidentiality has to do with protecting information. It is part of what’s called the CIA triad—Confidentiality, Integrity, and Availability.
* Authentication
  + Definition: Authentication is “the process or action of proving or showing something to be true, genuine, or valid.” In computing, it is “the process or action of verifying the identity of a user or process.” In cryptography, message authentication codes (MACs) are used to authenticate messages.
* Symmetric Key
  + Definition: Symmetric-key algorithms are those that use the same keys for both encryption and decryption. The keys are shared by two (or more) parties and used to maintain privacy and confidentiality in delivering the messages between the parties.
* Public Key
  + Definition: Public-key cryptography is also known as asymmetric cryptography, or Public Key Infrastructure (PKI). It’s a system that uses both a public key, which is, by definition, public, and can be widely known, and a private key, which is only known by the user. The functionality of PKI is two-fold—it serves to both authenticate and encrypt data.
* True Randomness
  + Randomness is when an event occurs completely unpredictably. There’s no pattern or logical order to the occurrence of the event. Computers can “randomly” generate numerical values, but rather than being true randomness it’s considered pseudorandomness.
* Plaintext
  + Definition: Plaintext is the format of a message before encryption or after decryption.
* HSM
  + Definition: HSM stands for Hardware Security Module. The HSM is a network computer built on specialized hardware that manages cryptographic operations, including key management, key exchange, encryption, etc. HSMs also generally have a security-focused OS, have limited network access that’s under strict control, and actively hide and protect cryptographic material.
* Integrity
  + Definition: Integrity is another element of the CIA triad. Integrity deals with the modification of information by unauthorized parties. Cryptography plays a hugely important role in ensuring the integrity of data. A few common ways to protect data integrity include hashing the received data and comparing it with the hash of the original, or digitally signing data using such things as GPG.
* Steganography
  + Definition: Steganography is the hiding of data within data. It is often used in partnership with cryptography to make data protection even more secure. It can be used in audio, video, images, and hashed text. Generally, the use of steganography is hidden from third-party users.
* Block Ciphers
  + Definition: A block cipher is an algorithm that operates on blocks, which are groups of bits of fixed length, using a symmetric key. It is commonly used to encrypt huge groupings of data. The block cipher used today is based on the iterated product cipher.
* Private Key
  + Definition: A private key is a key that is never shared with anyone. It makes up one of the keys used in public key encryption, also known as PKI. Private keys are paired with public keys to encrypt and decrypt messages.
* Kerckhoffs’s Principle
  + Definition: Kerckhoffs’s Principle is the idea that even if everything about a cryptosystem, other than the key, is public knowledge, the system should still be secure. It was originally stated by Auguste Kerckhoffs, and forms the basis for the maxim declared by Claude Shannon—that a person “ought to design [cryptographic] systems under the assumption that the enemy will immediately gain full familiarity with them.”
* Digital Signature
  + Definition: Digital signatures mathematically ensure the authenticity of documents or digitally transmitted messages. They are commonly used in different applications in which it is important to detect forgery or tampering, such as software distribution or financial transactions.
* SHR
  + Definition: SHR stands for Secure Hash Algorithms. As the name suggests, it’s a family of cryptographic hash functions. The Secure Hash Algorithms were created by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS). There are 4 of them: SHA-0, 1, 2, and 3.
* Non-Repudiation
  + Definition: Non-repudiation ensures that both the sender and receiver of data cannot deny that they sent or received the data. This is done through such things as digital signatures and other such measures of security.
* Cryptography
  + Definition: Cryptography is defined as a way of storing and transmitting data in a certain form, so that it can’t be intercepted by a third party (someone other than the sender and its intended recipient).
* Stream Ciphers
  + Definition: A stream cipher is a symmetric key cipher in which digits are combined with a keystream. (A keystream is a pseudorandom cipher digit stream.) The cipher uses the digits 0-9 and encrypts them using the corresponding keystream digits. Stream ciphers are also known as state ciphers, because the encryption of every digit depends on the current state of the cipher.
* The Enigma Machine
  + Definition: The enigma machine was invented by a German engineer by the name of Arthur Scherbius. It encrypts and decrypts messages using a series of mechanical rotors. Military and government organizations used them to communicate.
* Ciphertext
  + Definition: Ciphertext is the text of an encrypted message.
* GPG
  + Definition: GPG stands for GNU Privacy Guard. It’s a free hybrid-encryption software that uses both symmetric-key cryptography for speed, and public-key cryptography to ensure that key exchange is secure. It replaces Symantec’s PGP.
* Key Exchange
  + Definition: Key exchange is also known as key establishment. It’s the exchange of keys between two or more parties, in order to allow the use of cryptography to take place. If working with symmetric-key ciphers, both parties must have the same key. If working with asymmetric key ciphers, both parties will need the public key.