Encryption Cheat Sheet

Symmetric	**Asymmetric**	**Hashing**
DES/3DES	**RSA**	**MD5 128 bit**
AES	**El Gamal**	**SHA-1 160**
Twofish	**ECC Eliptic Curve**	HAVAL
Blowfish	**Diffie-Helman** **Key Exchange Algorithm**	PANAMA
Serpent	Paillier	
IDEA	Merkle-Helman	RIPEMD
/RC4’s RC5, RC6 **RC4 is a Stream Cipher**	Cramer-Shoup	Tiger
CAST		WHIRLPOOL

NOTE:

The text in red is what you focus on the most. You should be able to write out this chart prior to taking the exam.

Definitions:

Symmetric Key Encryption - A class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both decryption and encryption.

Asymmetric Key Encryption - A cryptographic approach, employed by many cryptographic algorithms and cryptosystems, whose distinguishing characteristic is the use of asymmetric key algorithms instead of or in addition to symmetric key algorithms.

Hybrid Cryptosystem - Combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem.

Public Key Cryptography - The distinguishing technique used in public key-private key cryptography is use of **asymmetric key algorithms** because the key used to encrypt a message is not the same as the key used to decrypt it.

Public Key Infrastructure (PKI) - a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates.
In cryptography, a **PKI** is an arrangement that binds public keys with respective user identities by means of a certificate authority (**CA**).

Certificate of Authority - An entity that issues digital certificates for use by other parties. It is an example of a trusted third party. CAs are characteristic of many public key infrastructure (PKI) schemes.

There are many commercial CAs that charge for their services. There are also several providers issuing digital certificates to the public at no cost. Institutions and governments may have their own CAs.

Digital Certificate – a **public key certificate** (or **identity certificate**) is an electronic document which utilizes a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

Digital Signature - A **digital signature** or **digital signature scheme** is a type of asymmetric cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless.

One-time Pad - is an encryption algorithm where the plaintext is combined with a random key or *"pad"* that is as long as the plaintext and used only once.

Block Cipher - A symmetric key cipher which operates on fixed-length groups of bits, termed *blocks*, with an unvarying transformation.

Steam Cipher - A symmetric key cipher where plaintext bits are combined with a pseudorandom cipher bit stream (keystream), typically by an exclusive-or (xor) operation. In a stream cipher the plaintext digits are encrypted one at a time, and the transformation of successive digits varies during the encryption.

Key Stream - A stream of random or pseudorandom characters that are combined with a plaintext message to produce an encrypted message (the ciphertext). The "characters" in the keystream can be bits, bytes, numbers or actual characters like A-Z depending on the usage case.

Brute Force Attack – Using all possible character combinations until a match for the password is found

Dictionary Attack – Using each entry in a word list until a match for the password is found.

Hashing – Applying a mathematical formula to a piece of text to get a shorter number or string.

One Way Hash – A hash where the original string the hash was derived from can not be easily found by a simple method.

Plain Text - The un-obfuscated or un-encrypted form of a string. Opposite of cipher text.

Reversible Encryption (Obfuscation) – Encryption that is easily reversed if the algorithm is known.

Salt – A number used to seed a hashing or encryption algorithm to add to the possible number of outcome ciphertexts.

Non-repudiation - the concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract. Although this concept can be applied to any transmission, including television and radio, by far the most common application is in the verification and trust of signatures.