Cheatography

Cryptography Cheat Sheet

by ipsec via cheatography.com/163245/cs/34186/

Symmetric (Block)

Name	*Key Size(bits)*	*Block Size(bits)*	*Rounds*
DES	56	64	16
3DES	56	64	16
AES	128,192,256	128	10,12,14
IDEA	128	64	8
Skipjack	80	64	32
Blowfish	32-448	64	16
Twofish	1-256	128	16
Camellia	128,192,256	128	18,24
RC2	1-128 (40 min)	64	18
RC5	1-2048	32,64,128	1-255
RC6	Variable (128,192,256)	32,64,128	20
XTEA	128	64	64

Symmetric (Stream)

Name	*Key Size(bits)*	*Rounds*	*Notes*
RC4	1-2048	1	40 bit key min, SSL, Web, WiFi
RCA	1-256	1-255	
FISH			Lagged Fibonacci PRNG, Data XOR'd w/ key
PIKE			FISH improvement to plaintext vulnerabilities, most common stream
ChaCha	256 bit key, 64 bit nonce		3x faster than software, enabled AES and not sensitive to timing attacks

Asymmetric

Name	*Description*	*Notes*
RSA	Leverages prime # 1024-4096 key size 1 round	Most popular, provides auth/encrypt, auth via **digital signatures**
ECC	Leverages discrete logarithm	Provides auth/encrypt, faster than RSA, uses less resources (**like cell phones**), auth via digital signatures
El Gamal	Used in recent versions of PGP	Extension of Diffie, similar protection as RSA/ECC, usually the slowest
DSA	Used to verify signatures, used Key pair, verified w/ public key	FIPS 186 Standard
Knapsack	Used for encrypt	Considered insecure
Diffie Hellman	No auth, MITM proned	Provides a method for **key exchange** using a one-way function.

Block Cipher Modes (Symmetric)

	Name	*Description*
ECB	Electronic Code Book	🔓Most basic, weak, and unsecure. 🔓Each block processed separately. 🔓No Salt or IV is used and the same key will be used to encrypt each block.
CBC	Cipher Block Chaining	🔓Minor step up from ECB. 🔓Added IV for the first block. 🔓Results of encryption from the previous block is input into to encryption process of the current block.

Block Cipher Modes (Symmetric) (cont)

CFB	Cipher Feedback	Converts the block cipher into a self-synchronizing stream cipher. Current block takes output of the XOR ⊕ process vs from the cipher stage of the previous block *(difference between CFB and OFB).*
OFB	Output Feedback	Converts the block cipher to a synchronous stream output. Current block takes output from cipher stage vs from the output of the XOR process of the previous block *(diff between CFB and OFB).* The first stage takes the data blocks and X-ORs it with encrypted version of the IV value. The output of the 1st stage encryption is then feed into the next stage, and encrypted, with the output being X-OR'ed with the second block.
CTR	Counter Mode	Converts the block cipher into a stream cipher. Generates a counter value and a nonce, and encrypts this, in order to EX-OR with the plain text block. Advantage of CTR is that each block is processed independent of the others, facilitating ability to conduct parallel processing of blocks. i.e., feedback from other stages to feed into the current one is not required.

Cryptographic Hash

Name	*Hash Value (bits)*
MD2	128
MD4	128
MD5	128
MD6	1-512
SHA-1	160
SHA-2	256,384,512
SHA-3	Variable
SHA-256	256
SHA-512	512

Historical Ciphers

Name	*Description*
Pigpen	Mono- alphabetic substitution cipher that makes use of mapping plaintext characters to graphical characters rather than to alphabetic ones. i.e. A=(pick a symbol), vs A=(pick a letter). Disadvantage: once the mapping is known, it is difficult to keep the message secret.
Rail Code	Employs a method to scramble text by writing it in a sequence across a number of rails.
BIFID	Makes use of a grid and which maps the letters into numeric values.
Playfair	5 × 5 matrix containing the alphabet less the letter J. Cipher/decipher process consists of a set of rules outlining use of column and row combinations.
Morse Code	Encoding method, rather than a cipher, that works by translating characters into sequences of dots (.) and dashes (-)

Historical Ciphers (cont)	
Caesar	Mono-alphabetic substitution cipher known as "shift" cipher. Involves plaintext being replaced by a letter some fixed number of positions down the alphabet. i.e., a Caesar Cipher using a shift of +3 would mean a plaintext letter A would result in a ciphertext letter D (a shift of three positions to the right in the alphabet).
Vigenere	Polyalphabetic cipher that involves using a different mapping, based on a keyword, for each character of the cipher. An advantage of this type of cipher is that the same plaintext character is likely to be coded to different mappings, depending on the position of the keyword, making guessing more difficult.
One Time Pad	Cipher code mapping that is used only once. Advantage is it is essentially unbreakable, disadvantage is it takes lots of work as you'd have to generate the pad to be used, each time.
Four-s-quare Cipher	Uses four 5 × 5 matrices arranged in a square, are where each matrix contains 25 letters for encoding and decoding operations.
Enigma Machine	Used a polyalphabetic substitution cipher, which did not repeat within a reasonable time period, along with a secret key. For the cracking of the Enigma cipher, the challenge was thus to determine both the algorithm used and the key. Enigma's main weakness, though, was that none of the plain text letters could be ciphered as itself