SYMMETRIC BLOCK CIPHERS

NAME	KEY SIZE	BLOCK SIZE	ROUNDS	ALGORITHM
DES	56 BIT	64 BITS	16 ROUNDS	FEISTEL
3DES (Runs DES 3 times)	56 BIT	64 BITS	16 ROUNDS	FEISTEL
AES	128,192, & 256 BITS	128 BITS	10 (128), 12 (192), 14 (256) ROUNDS	SUBSTITUTION- PERMUTATION, Rijyndael cipher
BLOWFISH (1993 by Bruce Schneider, Key expansion and encrypion data)	32 TO 448 BITS	64 BITS	16 ROUNDS	FEISTEL, in BCrypt, CrashPlan, Cryptodisk, DriveCrypt
TWO FISH (Bruce Schneider, Neil Ferguson, design to replace DES)	UP TO 256 BITS	128 BLOCK	16 ROUNDS	FEISTEL
SKIPJACK (Design by NSA for the Clipper Chip)	80 BITS	64 BITS	32 ROUNDS	UNBALANCE FEISTEL
IDEA (by James Massey & Xuejia Lai)	128 BITS	64 BITS	8 Rounds	Lai-Massey Scheme
CAST	128 OR 256 BITS	64 BITS	12 < 80 - 16>80	PGP, 8 bit rounds
TEA (by David Wheeler and Roger Needham)	128 BITS	64 BITS	64 ROUNDS	FEISTEL
SHARK (by Vincent Rijmen, Joan Daemen, Erick De Win)	128 BITS	64 BITS	6 ROUNDS	
RC5 & RC6 (Faster version of RC5)	up to 2048	32, 64, 128 BITS	up to 255	
SERPENT (Ross Anderson, Eli Biham, Lars Knudesen)	128,192, & 256 BITS	128 BITS	32 ROUNDS	SUBSTITUTION- PERMUTATION

SYMMETRIC ALGORITHM METHODS
IV: INTIALIZING VECTOR (Used with below ↓)
Nonce-Generated IV/Counter IV/Fixed IV/Random IV （↓）

CBC: CYPHER BLOCK CHAINING

CTR: Counter (Stream)

CFB:CIPHER FEEDBACK

OFB: OUPUT FEEDBACK (Stream)

ECB:ELECTRONIC CODE BOOK - each plaintext block encrypts to same length cipher block

PCBC: PROPAGATING CIPHER BLOCK CHAINING - used as a federal standard

ASYMETRIC CIPHERS			
RSA	Leverages prime number characteristics, 1024-4096 bit variable key size, 1 round		Most Popular / provides authentication and encryption / authentication through digital signatures
ECC	Leverages discrete logarithm characteristics	provides authentication and encryption/ faster than RSA / Uses less resources than RSA (Used in smaller devices like smartphones) / authentication through digital signatures	
El Gamal	Used in recent versions of PGP		Extension of Diffie Hellman (DH)/ Similar level of protection as RSA and ECC/ usually the slowest
DSA	A Federal Information Processing Standard for digital signatures (FIPS 186)		
Diffie Hellman (DH)	No Authentication /vulnerable to Man in the middle attacks		

FIPS STANDARDS	Acronyms
FIPS 180-2: Secure Hash Algorithm (SHA-1)	
FIPS 140: Define 4 security levels	OCSP – Online Certificate Status Protocol
FIPS 186: Digital Signatures	
FIPS 197: AES	
FIPS 201: Identity Verification	
FIPS 198: Hash-based Message Authentication Code (HMAC)	

KEY EXCHANGE ALGORITHMS
Diffie Hellman (DH)
Menezes-Qu-Vanstone (MQV)
Key Exchange Algorithm (KEA)
Elliptic Curve DH (ECDH)

RANDOM NUMBER GENERATOR TYPES
Table lookup generators
Hardware generators
Algorithmic (software) generators

Standards		
PKCS #1	RSA Cryptography Standard	
PKCS #3	Diffie–Hellman Key Agreement Standard	
PKCS #5/RFC 2898	Password-based Encryption Standard	
PKCS #8	Private-Key Information Syntax Standard	
PKCS #13	Elliptic Curve Cryptography Standard	
PKCS #14	Pseudo-random Number Generation	
PKCS #15	Cryptographic Token Information Format Standard	
RFC 1510	Kerberos Network Authentication Service (V5)	
RFC 1321	Message Digest 5 (MD5) hash	
RFC 2104	Hash-based Message Authentication Code (HMAC)	
RFC 3174	Secure Hash Algorithm (SHA-1)	
RFC 2040/PKCS#7	Block padding	
NIST 800-38A	CBC (Cipher Block Chaining) cipher mode	

NSA SUITE B ALGORITHMS
1: AES
2: AES with Galois/Counter Mode **Symmetric Encryption**
3: Elliptic-Curve DSA (ECDSA) **Digital Signatures**
4: Eliptic-Curve Diffie-Hellman (ECDH) **Key Agreement**
5: SHA2 (SHA256 - SHA384) **Message Digest**

Secure Channel
OCB: Fast but Patent issues
CCM: Slower than OCB but no known Patent issues
CWC: Speed improvement on CCM/universal hashing/ no patent issues
GCM: NIST standard block cipher mode/ no patent issues/ improvement on CWC

HASH FUNCTION		
MD5	128 BIT HASH, RFC 1321	
MD6	SUBMITED TO THE NIST SHA-3 COMPETITION	
SHA	160 bit hash, SHA-1, SHA-2(SHA-224, SHA-256, SHA-384, SHA-512), SHA3.	message digests - fixed length block of data after a hash function
FORK 256	USES A 512 BITS BLOCKS/ 256 bit Hash Value	
RIPEMD-160	160 BIT HASH, EXIST 128, 256 AND 320 VERSIONS	

GOST	DEFINED BY RUSSIAN NATIONAL STANDARD, 256 BITS OUTPUT	
TIGER	192 BITS HASH FUNCTION	
MAC & HMAC	A MAC USESES A BLOCK CIPHER IN CBC MODE TO IMPROVE INTEGRITY	

WIFI ENCRYPTION	
WEP (Wired Equivalent Privacy)	RC4 (128 bits or 256 to secure data and CRC-32 for checksum.
WPA Wi-Fi	PSK (Preshared Key & TKIP)
WPA2	802.1x, introduces CCMP (Counter Mode with Cipher Block Chaining)

NUMBER THEORY
PRIME NUMBERS: any number whose factors are 1 and itself only.
CO-PRIMES: A number that has no factors in common with another number.
EULER'S TOTIENT: Part of RSA.
MODULUS OPERATOR: is the reminder of divide A by N
FIBONACCI NUMBERS: adding the last 2 numbers create next
BIRTHDAY PARADOX: Related to hashes and collision.
BIRTHDAY ATTACK: Brute force attack against hashes.

LINEAR CONGRUENTIAL GENERATORS
The algorithm is: **$X_{n+1}=(aX_n+c) \bmod m$** where n>0
LAGGED FIBONACCI GENERATOR (LFG)
formula : $y= X^k+X^j+1$. can be Additive LFG, Multiplicative LFG or Two-tap LFG
BLUM BLUM SHUB
The algorithm is: **$X_{n+1}=X_n^2 \bmod m$**
YARROW
BY Bruce Schneider, john Kesley & Niels Ferguson, supplanted by Fortuna
FORTUNA
Group of PRNGs. 3 main components: generator, entropy accumulator and seed file.
DIFFIE HELLMAN
Use to share a key over insecure channel.
RSA (Rivest Shamir Adleman)
relationship with prime numbers, security derives from large prime numbers
encryption : **$=M^e \% n$** decryption: **$P=C^d \% n$**
MENEZES-QU-VANSTONE
is a protocol for key agreement base on diffie hellman, IEEE P1363
Elliptical Curve (EC): $y^2=x^3 + Ax + B$
SYMMETRIC

SYMMETRIC DECRYPTION: P = E(k,c)
SYMMETRIC ENCRYPTION: C = E(k,p)

Variables		
Ke	secret key	
E	encryption	
D	Decryption	
m	Message	
a	*message authentication code*	
h	MAC function	
P	public key	PKI
S	secret key	PKI
s	signature	
v	verification key	
P	plain text	padding
C	cipher text	padding
l (P)	length of Plaintext in bytes	padding
b	block size	padding
K	number of blocks	padding
K_0	Key Stream	
$\oplus$	XOR	
M	blocks in total	Chances of a Collision expect the first duplicate ciphertext block
n	block size of the block cipher	Chances of a Collision expect the first duplicate ciphertext block
h	iterative hash function	
T	tag	MAC

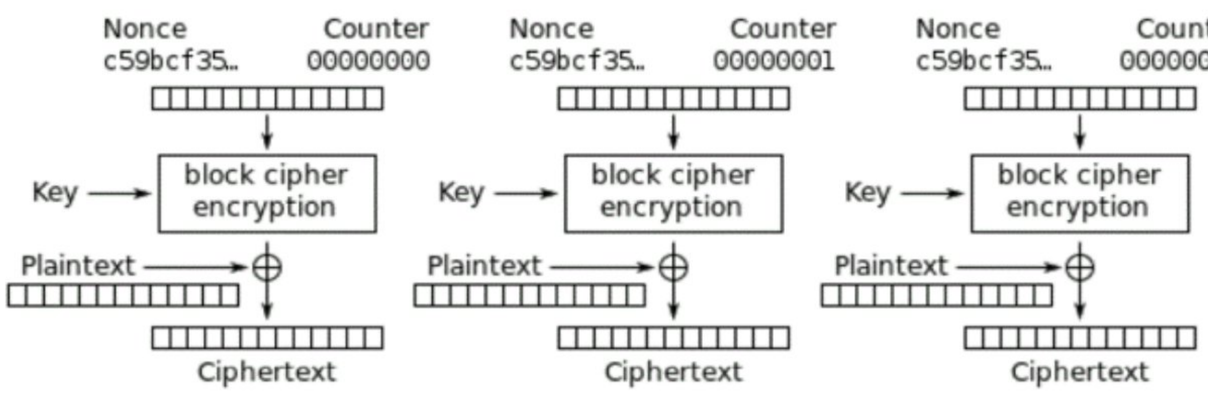
NOTABLE DATES IN TIME		
1466	Cipher disk invented by Leon Alberti	
1553	Vigenere Cipher invented by Giovan Battista Bellaso	
1854	Playfair Cipher invented by Charles Wheatstone	
1863	1st successful attack on the Vigenere cipher published by Friedrich Kasiski	
1918	ADFGVX Cipher invented by Colonel Fritz Nebel	
1918	Enigma Machine invented in 1918 by Arthur Scherbius	
WWII	Enigma Machine used by the Germans	
1977	RSA invented by Ron Rivest, Adi Shamir, and Len Adleman	
1988	X.509 first use	
1991	DSA filed and attributed to David Kravitz | US Patent 5,231,668	

1993	DSA adopted by US Government with FIPS 186	
1993	FISH (Fibonacci Shrinking) published by Siemens	
1995	TIGER designed by Ross Anderson	
2001	AES (Rijndael) announced as replacement for DES | FIPS 197	

Historical Ciphers	
Mono-Alphabet Substitution Ciphers: (Single Alphabet)	
Atbash	Reverses the alphabet (A becomes Z, B becomes Y ...)
Ceasar	Choose some number by which to shift each letter of the message. (right is "+" | left is "-" | A "+2" = C | C "-1" = B)
ROT-13	Rotate all characters 13 letters through the alphabet (A becomes N, B becomes O ...)
Scytale	Use of a rod of a certain length to create/encrypt a message, and same rod must be used to read/decrypt the message by the recipient
Multi-Alphabet Substitution	add complexity by adding alphabets to be used for the substitution rounds. Example: We are using three alphabets to do the shifting, each represented by a "+" or a "-" value. When we run out of alphabets, we start over again with the first one, effectively "roundrobining" through the text until it is all shifted.
A DOG (+1-2+1)	
B BPH	
The cipher disk	a physical device used to encrypt. Invented by Leon Alberti in 1466. The cipher disk was polyalphabetic; each time you turned the disk, you used a new cipher.
The Vigenère cipher	invented in 1553 by Giovan Battista Bellaso, but is named for Blaise de Vigenère who developed a stronger version of the cipher. It is a method of encrypting by using a series of interwoven Caesar ciphers based on the letters of a keyword. It is considered a polyalphabetic cipher system. Friedrich Kasiski published the first successful attack against the Vigenère cipher in 1863.
The Playfair Cipher	invented by Charles Wheatstone in 1854. Uses a five-by-five table containing a keyword or key phrase. To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill in the remaining spaces with the rest of the letters of the alphabet in order. The technique encrypts pairs

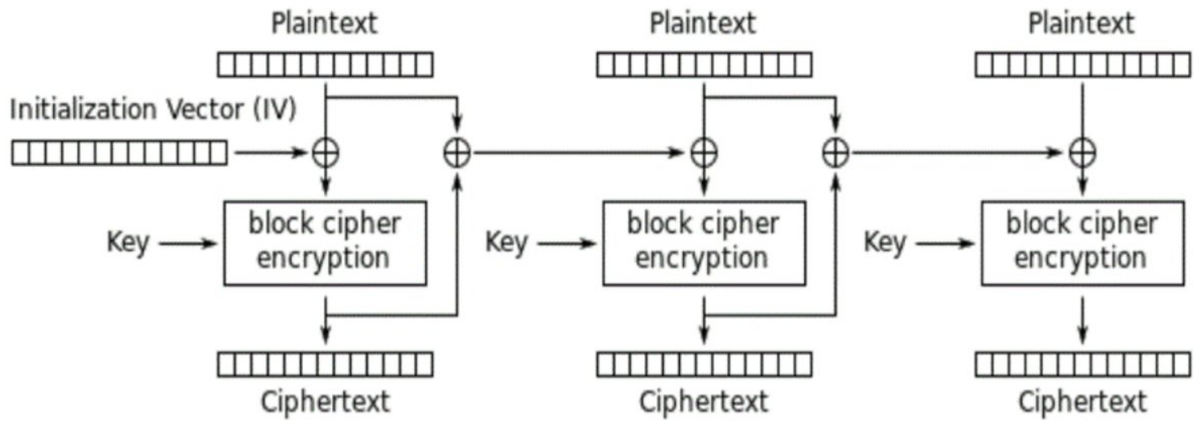
	of letters (digraphs), instead of single letters as in the simple substitution cipher. The Playfair is m n p q s t u v w x
The ADFGVX Cipher	The key for this algorithm is a six-by-six square made up of the letters ADFGVX forming the outer row and column, the rest of the table is comprised of the letters of the alphabet and the numbers 0 through 9 distributed randomly in the square.
The ENIGMA Machine	a multi-alphabet substitution cipher using machinery to accomplish the encryption. In World War II, the Germans used this as an electromechanical rotor-based cipher system.
Affine cipher	The Affine cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter.

- Like OFB, Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter".



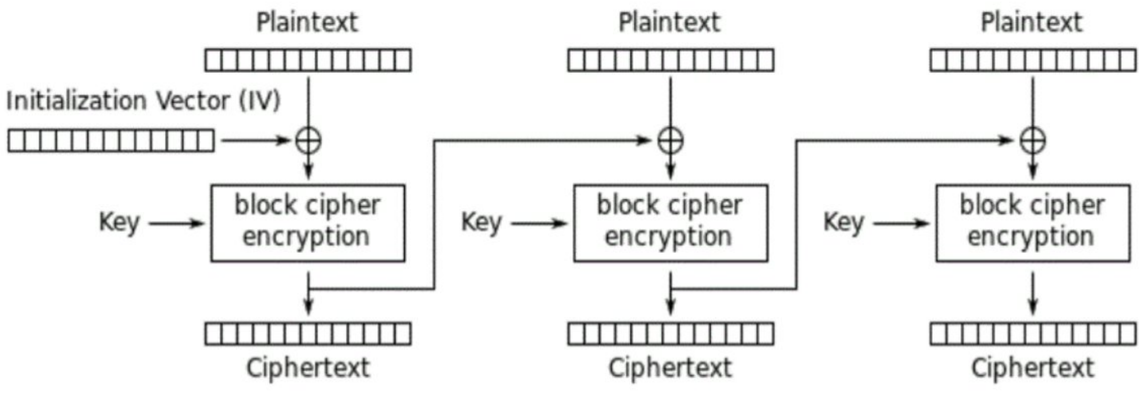
Counter (CTR) mode encryption

Propagating Cipher Block Chaining (PCBC) – Each block of plaintext is XORed with the XOR of the previous plaintext block and the previous ciphertext block before being encrypted. As with CBC mode, an initialization vector is used in the first block.



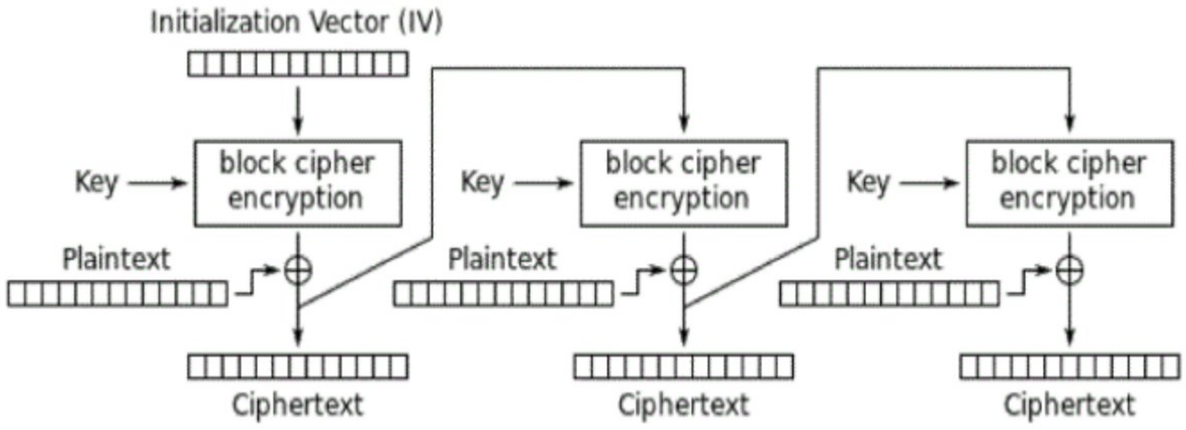
Propagating Cipher Block Chaining (PCBC) mode encryption

Cipher Block Chaining (CBC) – Each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.



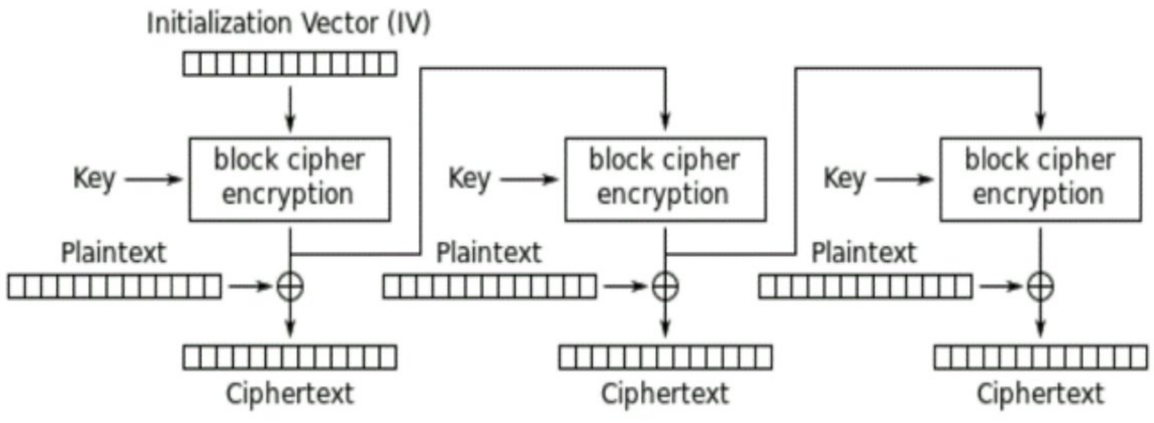
Cipher Block Chaining (CBC) mode encryption

Cipher Feedback (CFB): Allows encryption of partial blocks rather than requiring full blocks for encryption. This eliminates the need to pad a block like in CBC.



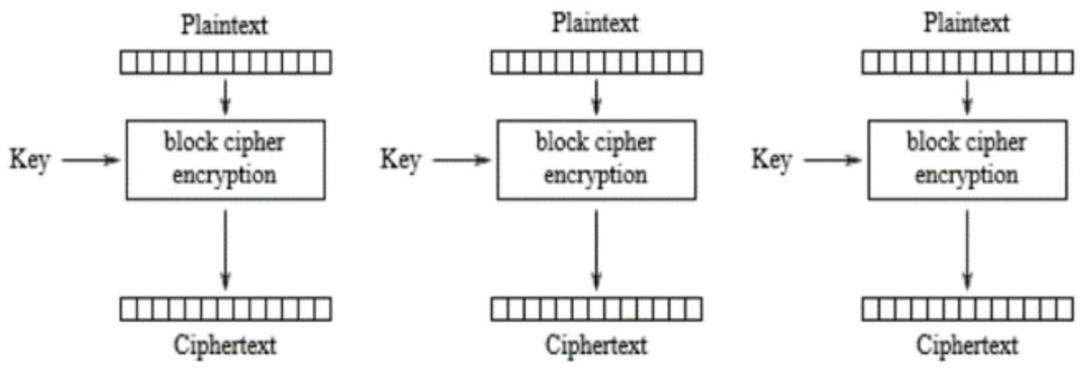
Cipher Feedback (CFB) mode encryption

The Output Feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext.



Output Feedback (OFB) mode encryption

Electronic Code Book (ECB) – Each block is encrypted independently, BUT identical plaintext blocks are encrypted into identical ciphertext blocks



Electronic Codebook (ECB) mode encryption