Operates On	Name	Authors
Block	**AES**	
Block	**SERPENT**	Ross Anderson, Eli Biham, Lars Knudesen
Block	**TWO FISH**	Bruce Schneider, Neil Ferguson, design to replace DES
Block	**RC5 & RC6**	
Block	**IDEA**	James Massey & Xuejia Lai
Block	**TEA**	David Wheeler and Roger Needham
Block	**SHARK**	Vincent Rijmen, Joan Daemen, Erick De Win
Block	**CAST**	
Block	**BLOWFISH**	1993 by Bruce Schneider, Key expansion and encryption data
Block	**DES**	
Block	**3DES**	
Block	**SKIPJACK**	
Stream	**RCA**	
Stream	**RC4**	
Stream	**FISH**	
Stream	**PIKE**	

Key Size(s) in bits	Block Size(s) in bits
128,192, & 256	128
128,192, & 256	128
Up TO 256	128
Up to 2048	32, 64, 128
128	64
128	64
128	64
128 or 256	64
32 to 448	64
56	64
56	64
80	64
1-256	
2064 bit state size, 1-2048 bit key size	

Rounds
10 (128), 12 (192), 14 (256) ROUNDS
32 ROUNDS
16 ROUNDS
up to 255
8 Rounds
64 ROUNDS
6 ROUNDS
12 < 80 - 16>80
16 ROUNDS
16 ROUNDS
16 ROUNDS
32 ROUNDS
up to 255 rounds
1

Algorithm
SUBSTITUTION- PERMUTATION, Rijyndael cipher
SUBSTITUTION- PERMUTATION
FEISTEL
Lai-Massey Scheme
FEISTEL
PGP, 8 bit rounds
FEISTEL, in BCrypt, CrashPlan, Cryptodisk, DriveCrypt
FEISTEL
FEISTEL
UNBALANCE FEISTEL
Uses Lagged Fibonacci pseudorandom number generator. data stream XORed with the key
Revised version of FISH to address known plaintext attack vulnerabilities

Notes
Process flow: 1- Subbytes, 2- Shift rows, 3- Mix-columns, 4- Add round Key. In the fina
Faster version of RC5
Runs DES 3 times
Design by NSA for the Clipper Chip
Weak stream cipher/ used in SSL & Web / WIFI security/ RFC 7465 prohibits use in TLS
40 bit minimum key size recommended
FISH IMPROVEMENT
most widely used stream cipher

l (10th) round, there is no Mix-column

Name	Description
RSA	Leverages prime number characteristics, 1024-4096 bit variable key size, 1 round
ECC	Leverages discrete logarithm characteristics
El Gamal	Used in recent versions of PGP
DSA	A Federal Information Processing Standard for digital signatures (FIPS 186)
Diffie Hellman (DH)	No Authentication /vulnerable to Man in the middle attacks

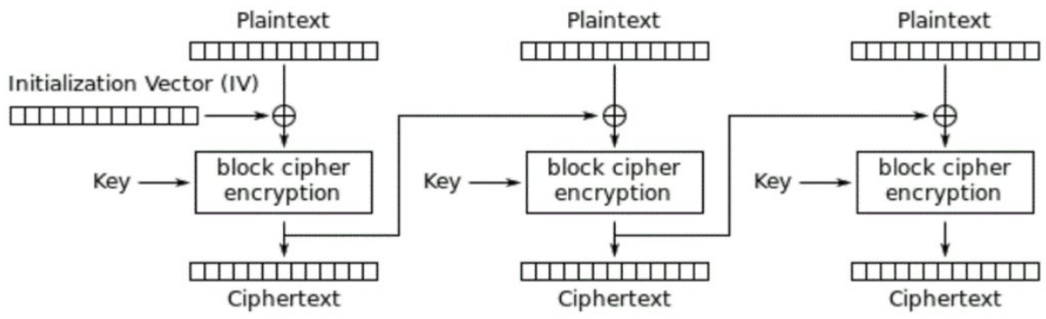
Notes
Most Popular / provides authentication and encryption / authentication through digital signatures
provides authentication and encryption/ faster than RSA / Uses less resources than RSA (Used in smaller devices like smartphones) / authentication through digital signatures
Extension of Diffie Hellman (DH)/ Similar level of protection as RSA and ECC/ usually the slowest

Block cipher modes	Can function on Stream
CBC: CYPHER BLOCK CHAINING	
CTR: COUNTER	**Yes**
CFB:CIPHER FEEDBACK	
OFB: OUTPUT FEEDBACK	**Yes**

Notes

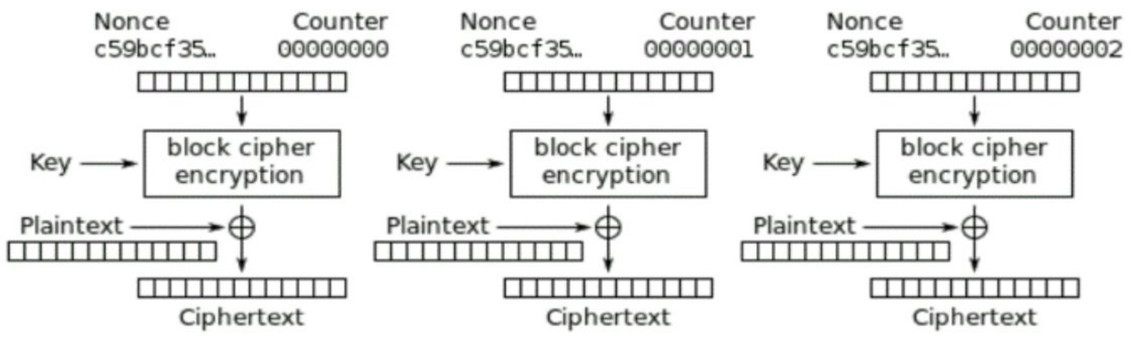
Diagram

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.



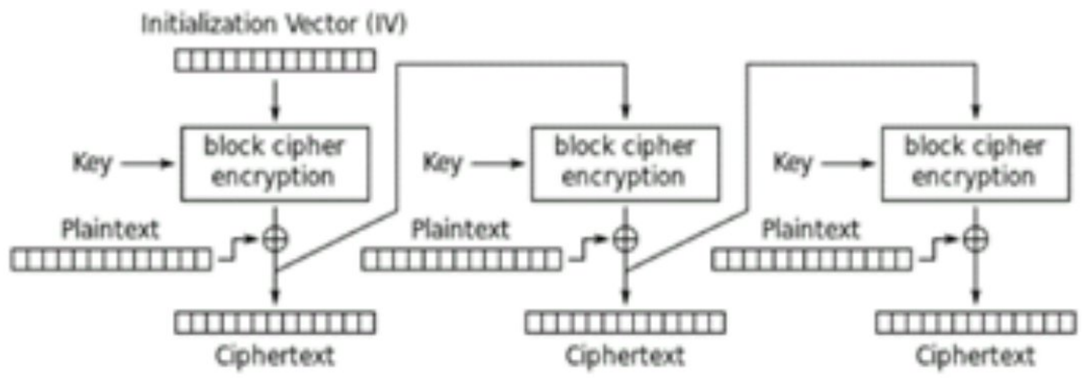
Cipher Block Chaining (CBC) mode encryption

- 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".



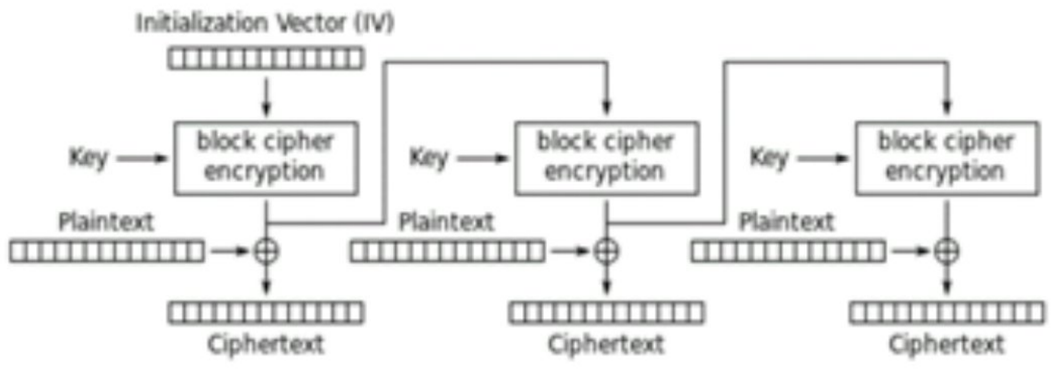
Counter (CTR) mode encryption

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.

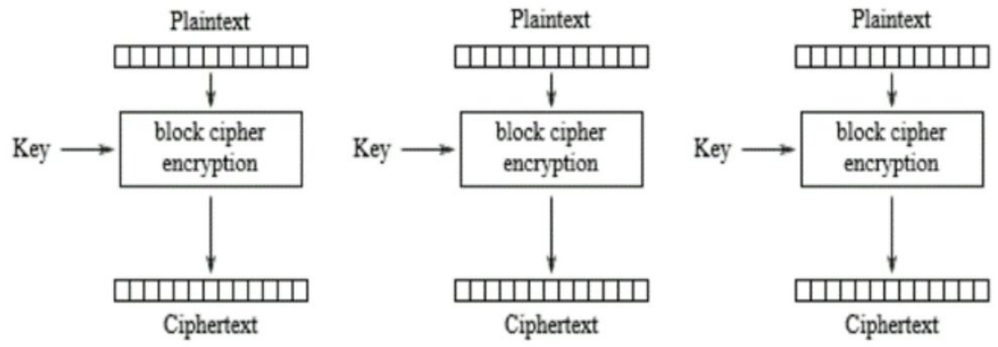


Output Feedback (OFB) mode encryption

ECB:ELECTRONIC CODE BOOK	
PCBC: PROPAGATING CIPHER BLOCK	CHAINING

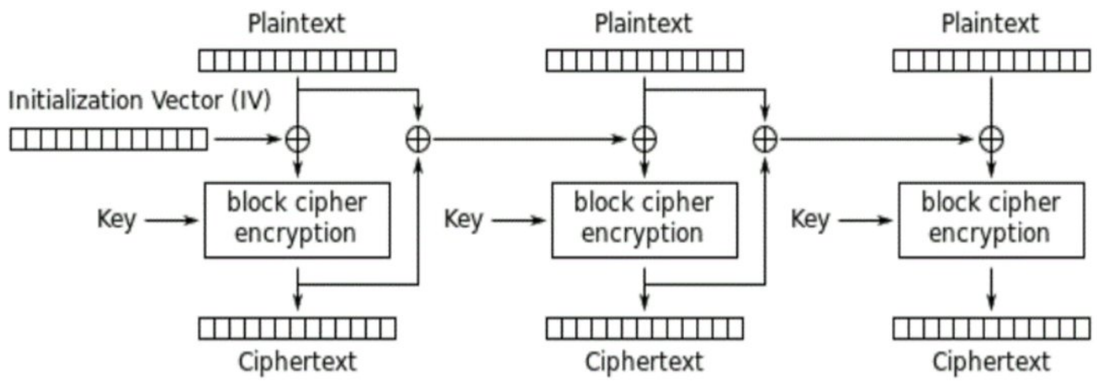
Simplest mode. Each plaintext block encrypts to same length cipher block. Same plaintext encrypts to same ciphertext.

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



Electronic Codebook (ECB) 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

Standard
FIPS 180-2: Secure Hash Algorithm (SHA-1)
FIPS 140: Define 4 security levels
FIPS 186: Digital Signatures
FIPS 197: AES
FIPS 201: Identity Verification
FIPS 198: Hash-based Message Authentication Code (HMAC)
PKCS #1
PKCS #3
PKCS #5/RFC 2898
PKCS #8
PKCS #13
PKCS #14
PKCS #15
RFC 1510
RFC 1321
RFC 2104
RFC 3174
RFC 2040/PKCS#7
NIST 800-38A

Description	
RSA Cryptography Standard	
Diffie–Hellman Key Agreement Standard	
Password-based Encryption Standard	
Private-Key Information Syntax Standard	
Elliptic Curve Cryptography Standard	
Pseudo-random Number Generation	
Cryptographic Token Information Format Standard	
Kerberos Network Authentication Service (V5)	
Message Digest 5 (MD5) hash	
Hash-based Message Authentication Code (HMAC)	
Secure Hash Algorithm (SHA-1)	
Block padding	
CBC (Cipher Block Chaining) cipher mode	

Date
1466
1553
1854
1863
1918
1918
WWII
1977
1988
1991
1993
1993
1995
2001

Historical Ciphers
Mono-Alphabet Substitution Ciph
Atbash
Caesar
ROT-13
Scytale
Multi-Alphabet Substitution
The cipher disk
The Vigenère cipher

Event
Cipher disk invented by Leon Alberti
Vigenere Cipher invented by Giovan Battista Bellaso
Playfair Cipher invented by Charles Wheatstone
1st successful attack on the Vigenere cipher published by Friedrich Kasiski
ADFGVX Cipher invented by Colonel Fritz Nebel
Enigma Machine invented in 1918 by Arthur Scherbius
Enigma Machine used by the Germans
RSA invented by Ron Rivest, Adi Shamir, and Len Adleman
X.509 first use
DSA filed and attributed to David Kravitz | US Patent 5,231,668
DSA adopted by US Government with FIPS 186
FISH (Fibonacci Shrinking) published by Siemens
TIGER designed by Ross Anderson
AES (Rijndael) announced as replacement for DES | FIPS 197

Description
Single Alphabet
Reverses the alphabet (A becomes Z, B becomes Y ...)
Choose some number by which to shift each letter of the message. (right is "+" | left is "-" | A "+2" = C | C "-1" = B)
Rotate all characters 13 letters through the alphabet (A becomes N, B becomes O ...)
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
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 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.
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
The ADFGVX Cipher
The ENIGMA Machine
Affine 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 significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. A typical 5x5 key square is below: (Any sequence of 25 letters can be used as a key, so long as all letters are in it and there are no repeats. Note that there is no 'j', it is combined with 'i'.) k e y w o r d a b c f g h i l m n p q s t u v w x
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.
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.
The Affine cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric eq simple mathematical function, and converted back to a letter.

Term/Variable	Definition
OCSP	Online Certificate Status Protocol
Message Digest	fixed length block of data, result of hash function
IV	Initialization Vector
Nonce	Generated IV/Counter IV/Fixed IV/Random IV（↓）
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	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.
Ke	secret key
E	encryption
D	Decryption
m	Message
a	message authentication code
h	MAC function
P	public key
S	secret key
s	signature
v	verification key
P	plain text
C	cipher text
l (P)	length of Plaintext in bytes
b	block size
K	number of blocks
K0	Key Stream
⊕	XOR
M	blocks in total
n	block size of the block cipher
h	iterative hash function
T	tag

KEY EXCHANGE ALGORITHMS
Diffie Hellman (DH)
Menezes-Qu-Vanstone (MQV)
Key Exchange Algorithm (KEA)
Elliptic Curve DH (ECDH)
NSA SUITE B ALGORITHMS
1: AES
2: AES with Galois/Counter Mode **Symmetric Encryption**
3: Elliptic-Curve DSA (ECDSA) **Digital Signatures**
4: Elliptic-Curve Diffie-Hellman (ECDH) **Key Agreement**
5: SHA2 (SHA256 - SHA384) **Message Digest**
Secure Channel
OCB
CCM
CWC
GCM
HASH FUNCTION
MD5
MD6
SHA
FORK 256
RIPEMD-160
GOST
TIGER
MAC & HMAC
WIFI ENCRYPTION
WEP (Wired Equivalent Privacy)
WPA Wi-Fi
WPA2

Fast but Patent issues
Slower than OCB but no known Patent issues
Speed improvement on CCM/universal hashing/ no patent issues
NIST standard block cipher mode/ no patent issues/ improvement on CWC
128 BIT HASH, RFC 1321
SUBMITED TO THE NIST SHA-3 COMPETITION
160 bit hash, SHA-1, SHA-2(SHA-224, SHA-256, SHA-384, SHA-512), SHA3.
USES A 512 BITS BLOCKS/ 256 bit Hash Value
160 BIT HASH, EXIST 128, 256 AND 320 VERSIONS
DEFINED BY RUSSIAN NATIONAL STANDARD, 256 BITS OUTPUT
192 BITS HASH FUNCTION
A MAC USESES A BLOCK CIPHER IN CBC MODE TO IMPROVE INTEGRITY
RC4 (128 bits or 256 to secure data and CRC-32 for checksum.
PSK (Preshared Key & TKIP)
802.1x, introduces CCMP (Counter Mode with Cipher Block Chaining)

RSA (Rivest Shamir Adleman)	relationship with prime numbers, security derives from large prime numbers	encryption : **=Me% n** decryption: **P=Cd % n**
Elliptical Curve (EC)		y2=x3 + Ax + B
Symmetric Encryption		DECRYPTION: P = E(k,c) ENCRYPTION: C = E(k,p)

RANDOM NUMBER GENERATORS TYPES
Table lookup generators
Hardware generators
Algorithmic (software) generators
Algorithmic Pseudo Random Number Generator
LINEAR CONGRUENTIAL GENERATORS
LAGGED FIBONACCI GENERATOR (LFG)
BLUM BLUM SHUB
YARROW
FORTUNA

Description
The algorithm is: **Xn+1=(aXn+c)Mod m** where n>0
formula : y= Xk+Xj+1. can be Additive LFG, Multiplicative LFG or Two-tap LFG
The algorithm is: **Xn+1=Xn2 Mod m**
BY Bruce Schneider, john Kesley & Niels Ferguson, supplanted by Fortuna
Group of PRNGs. 3 main components: generator, entropy accumulator and seed file.