Symmetric Ciphers

Name	Authors	Key Size(bits)	Block Size(bits)	Rounds	Algorithm	Notes
AES		128 192 256	128	10 (*128*) 12 (*192*) 14 (*256*)	Substitution-Permutation, Rijyndael Cipher	
SERPENT	Ross Anderson, Eli Biham, Lars Knudsen	128 192 256	128	32	Substitution-Permutation	
TWOFISH	Bruce Schneider, Neil Ferguson	Up to 256	128	16	Feistel	Designed to replace DES
RC4		1-2048	**STREAM**	1		40-bit minimum key size recommended SSL, Web, WiFi RFC
RC5 **RC6**		1-2048	32 64 128	Up to 255		RC6 is a faster version of RC5
IDEA	James Massey, Xuejia Lai	128	64	8	Lai-Massey Scheme	
TEA	David Wheeler, Roger Needham	128	64	64	Feistel	
SHARK	Vincent Rijimen, Joan Daemen, Erick De Win	128	64	6		
CAST-128 **CAST-256**		40-128	64	12(<80) 16(>80)	PGP	8-bit rounds
BLOWFISH	Bruce Schneider	32-448	64	16	Feistel	BCrypt, CrashPlan, Cryptodisk, DriveCrypt
DES		56	64	16	Feistel	
3DES		56	64	16	Feistel	Runs DES 3 times
SKIPJACK		80	64	32	Unbalanced Feistel	Designed by NSA for Clipper Chip
RCA		1-256	**STREAM**	Up to 255		
FISH			**STREAM**		Lagged Fibonacci PRNG, Data XOR'd with key	
PIKE			**STREAM**			FISH improvement to address plaintext vulnerabilities, most common stream cipher used

Asymmetric Ciphers

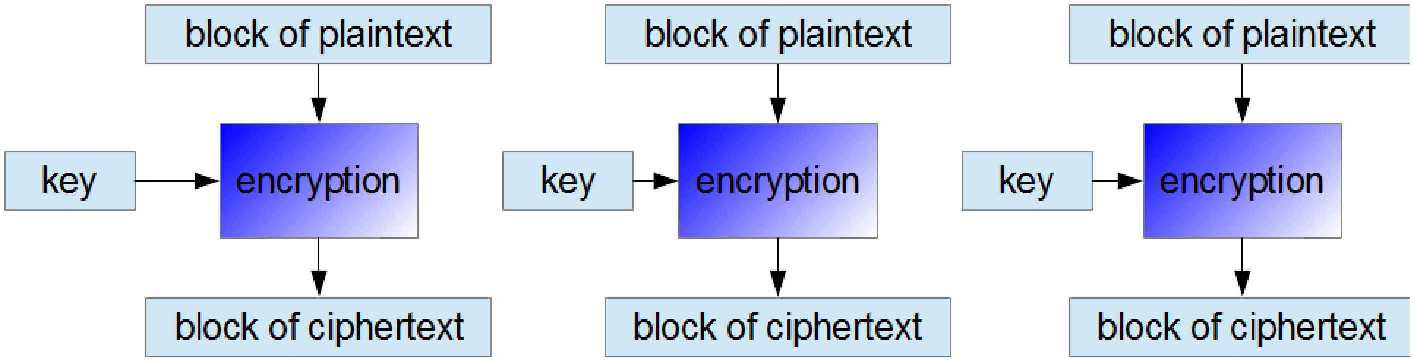
Name	Authors	Description	Notes
RSA	Ron Rivest, Adi Shamir, Leonard Aldeman	Leverages prime number characteristics, 1024-4096 key bit size, 1 round	Most popular, provides authentication and encryption, authentication through digital signatures
ECC		Leverages discrete logarithm characteristics	Provides authentication and encryption, faster than RSA, uses less resources than RSA (like cellphones), authentication through digital signatures
El Gamal		Used in recent versions of PGP	Extension of Diffie-Hellman, similar level of protection as RSA & ECC, usually the slowest
DSA		Federal Information Processing Standard for digital signatures (FIPS186)	
Diffie-Hellman		No authentication and vulnerable to MITM attacks	

Block Cipher Modes

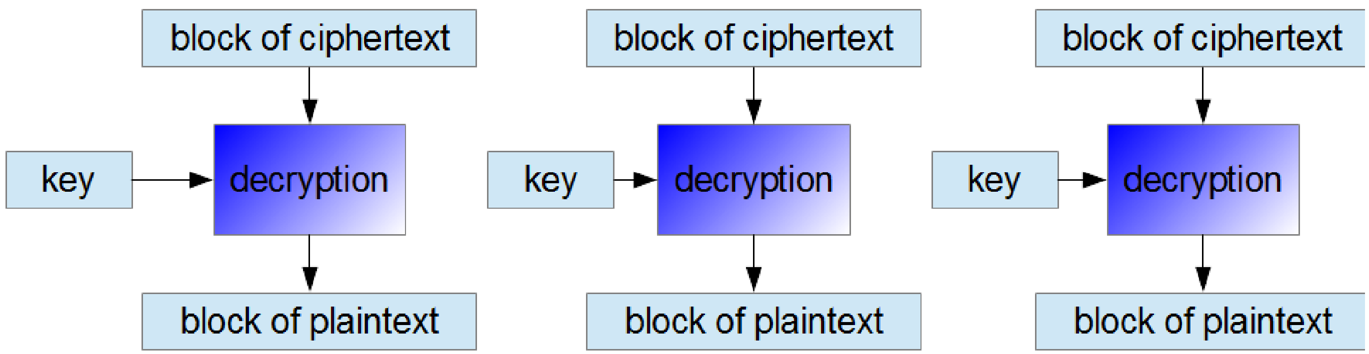
ECB (Electronic Codebook) Mode:

- Simplest mode of encryption. Each plaintext block is encrypted separately. Each ciphertext block is decrypted separately.

ECB Encryption



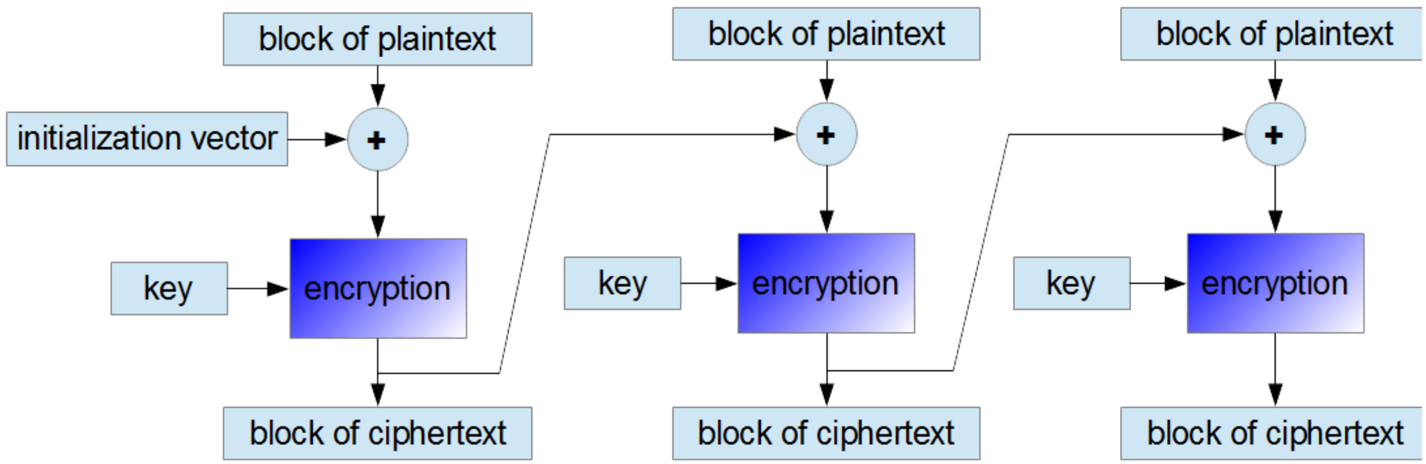
ECB Decryption



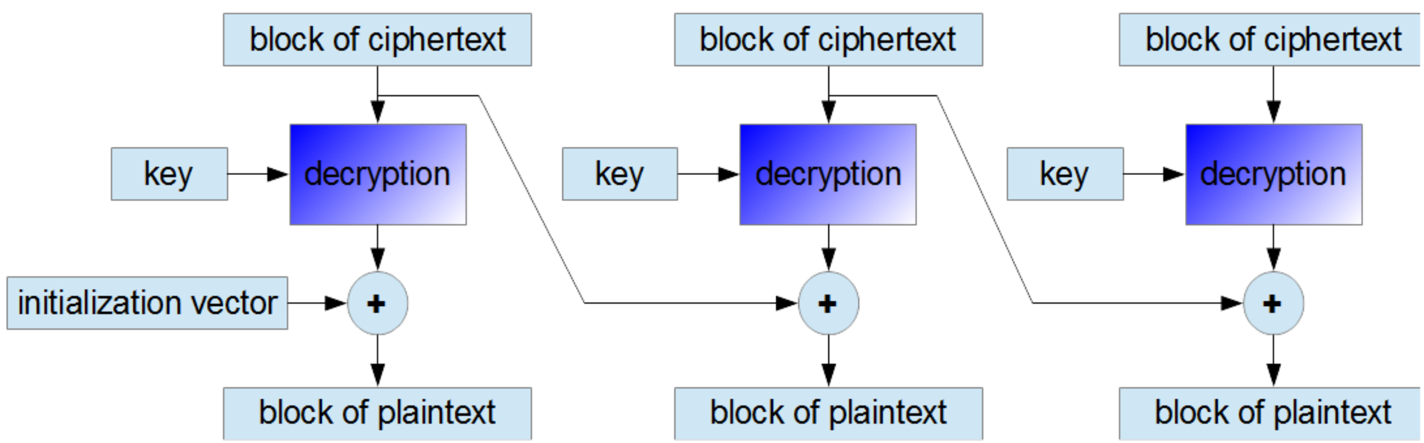
CBC (Cipher-Block Chaining) Mode:

- This mode is about adding XOR of each plaintext block to the ciphertext block that preceded it. The result is encrypted using the cipher algorithm in the usual way. As a result, every subsequent ciphertext block depends on the previous one. The first plaintext block is added XOR to a random initialization vector (IV). The vector has the same size as the plaintext block.
- If one bit of a plaintext message is damaged, all subsequent ciphertext blocks will be damaged and it will never be possible to decrypt the ciphertext received from this plaintext.
- If one bit of ciphertext is damaged, only two received plaintext blocks will be damaged.

CBC Encryption



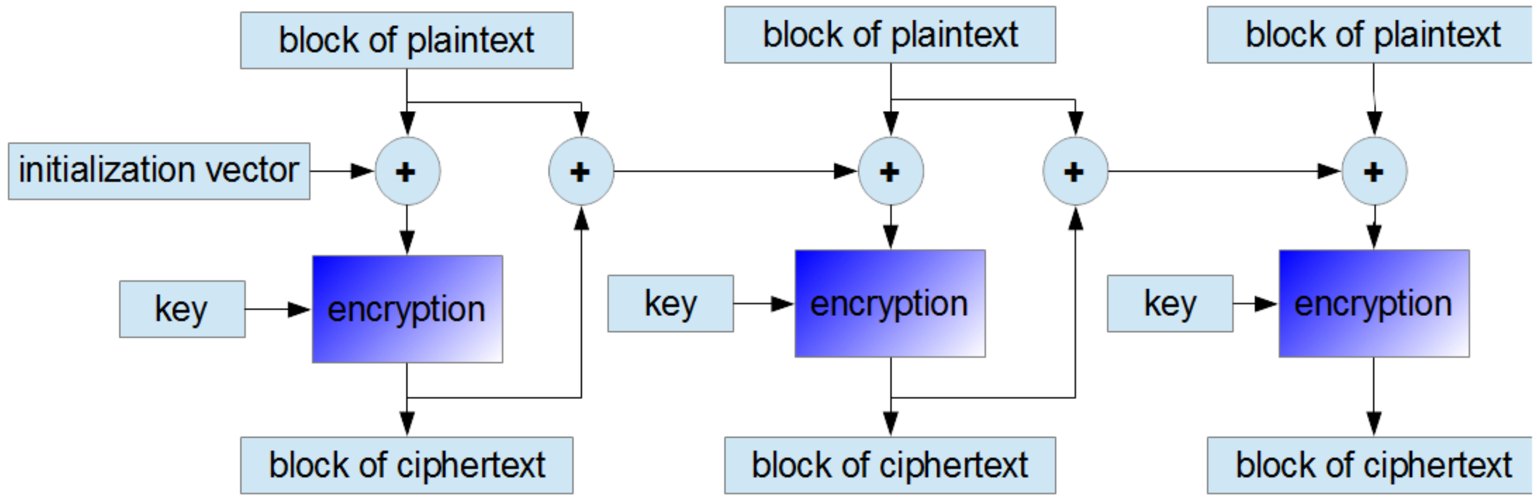
CBC Decryption



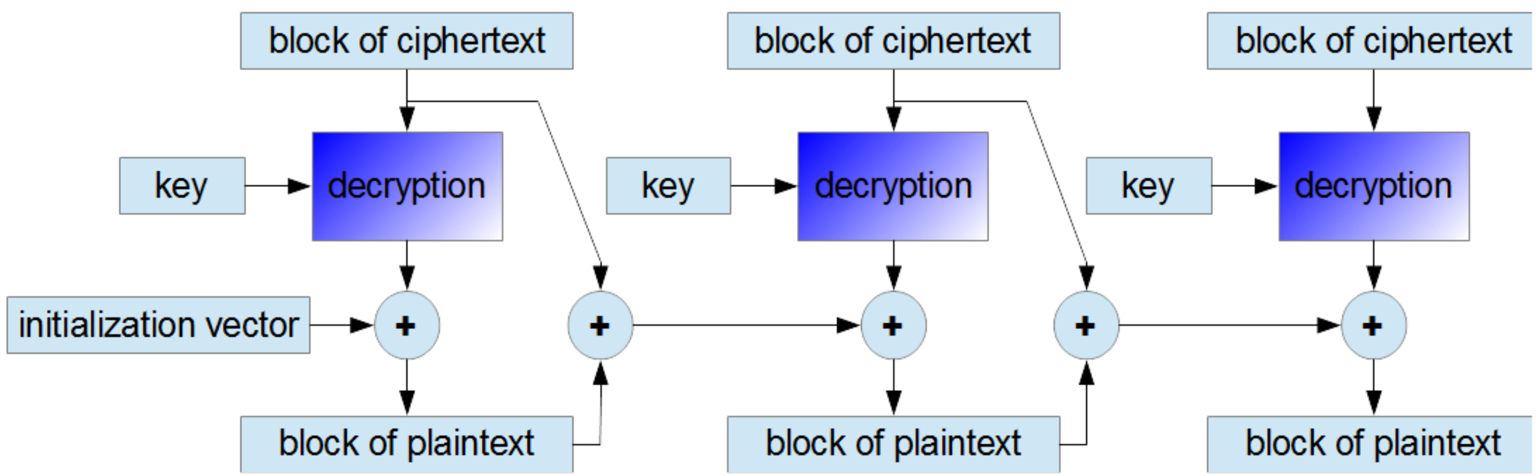
PCBC (Propagating or Plaintext Cipher-Blocking Chaining) Mode:

- Like CBC mode.
- Mixes bits from previous ciphertext and plaintext blocks before encrypting them.
- If one ciphertext bit is damaged, the next plaintext block and all subsequent blocks will be damaged and unable to decrypt.

PCBC Encryption



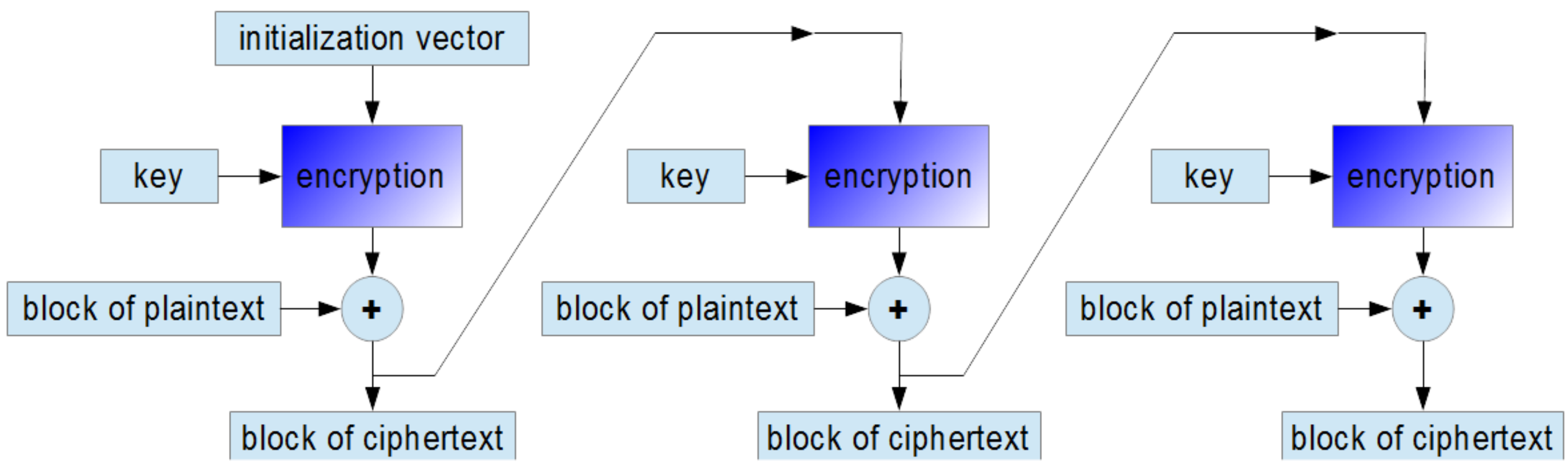
PCBC Decryption



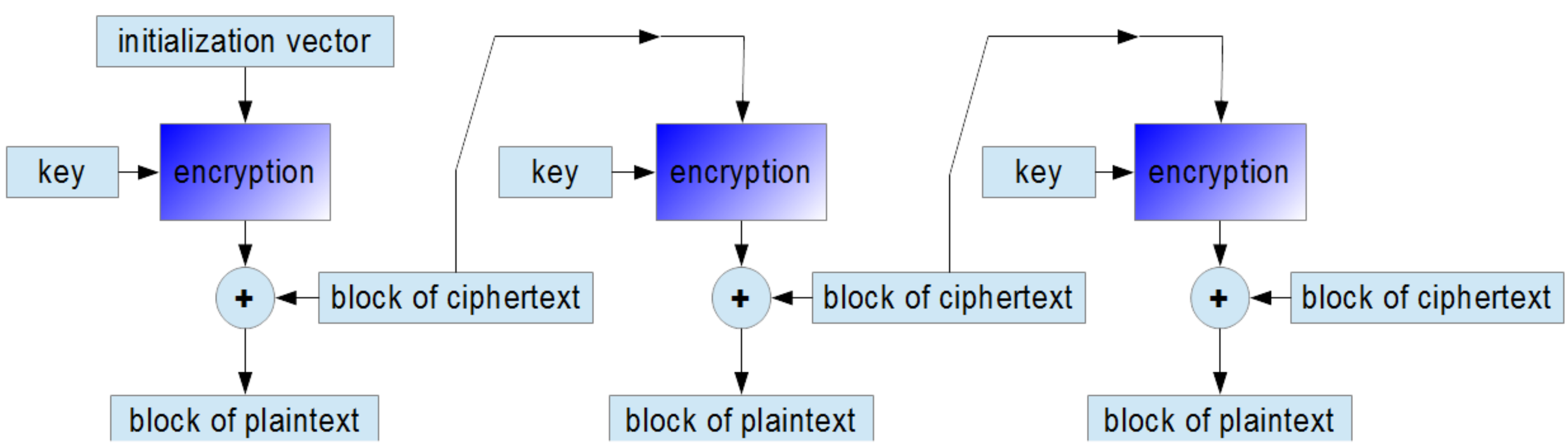
CFP (Cipher Feedback) Mode:

- CFP is like CBC.
- Ciphertext from the previous round is encrypted each round and then add the output to the plaintext bits.
- If one bit of plaintext message is damaged, the corresponding ciphertext block and all subsequent cyphertext blocks will be damaged.
- If one ciphertext bit is damaged, only two received plaintext blocks will be damaged.

CFP Encryption



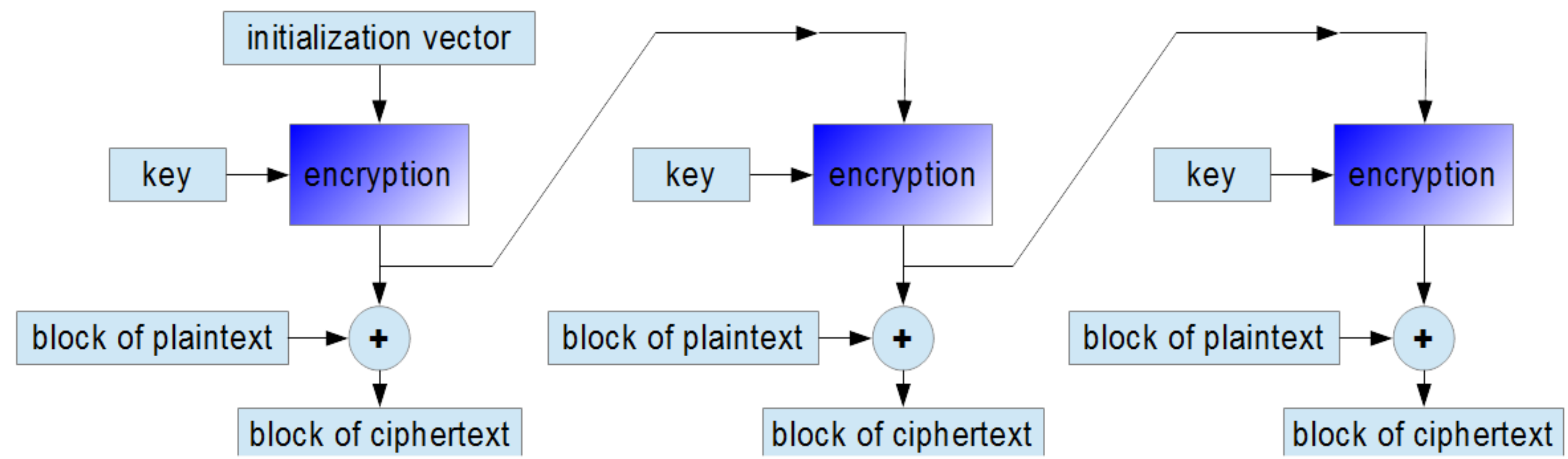
CFP Decryption



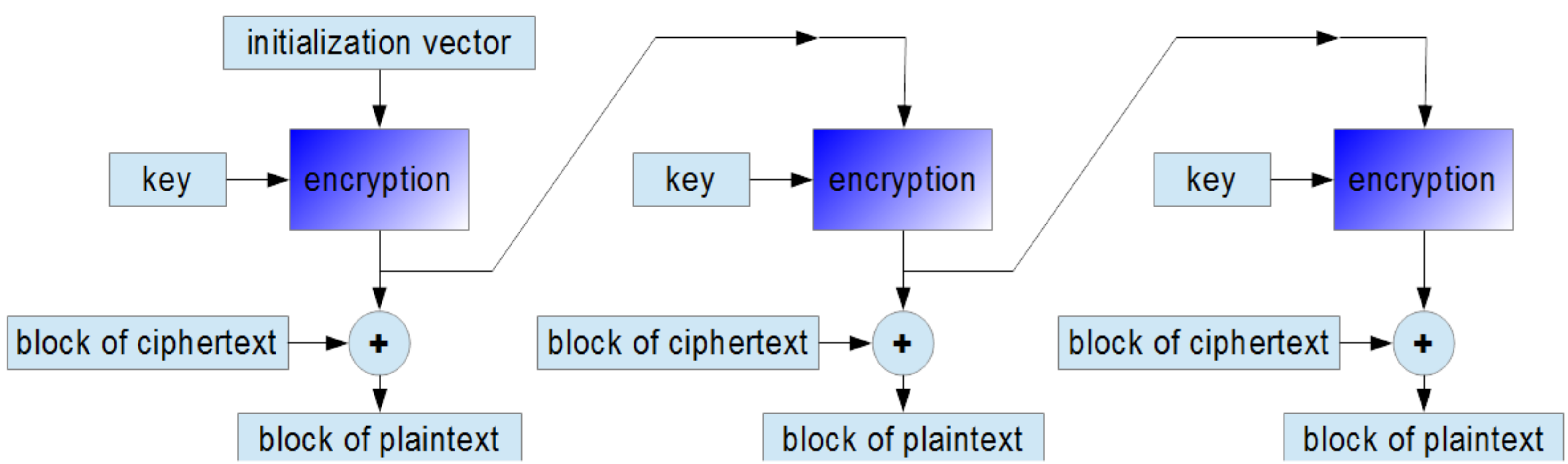
OFB (Output Feedback) Mode:

- Can function on stream and create keystreams.
- If one bit of plaintext or ciphertext is damaged, only one corresponding ciphertext or plaintext bit is damaged.
- Drawback is that the repetition of encrypting the initialization vector may produce the same state that has occurred before.

OFB Encryption



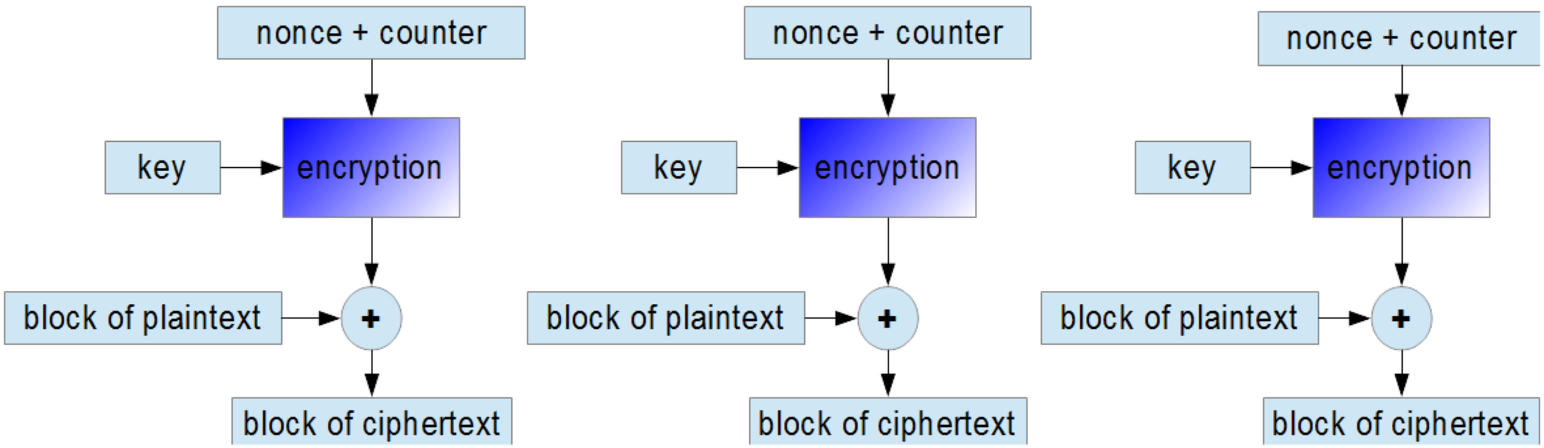
OFB Decryption



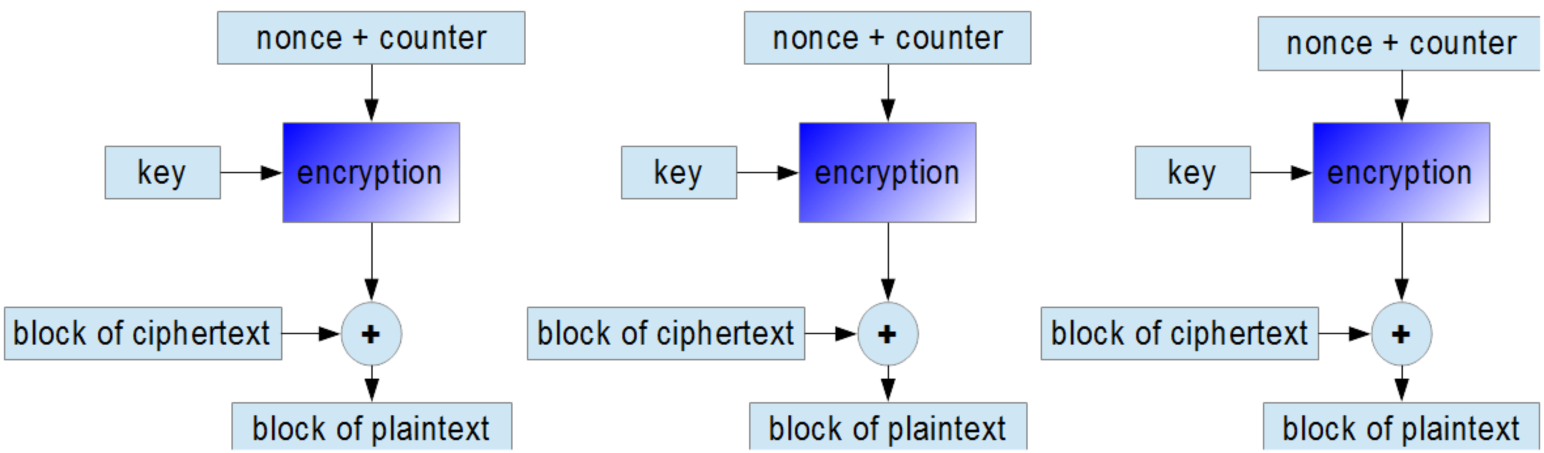
CTR (Counter) Mode:

- Can function on streams and create keystreams.
- Streams are created regardless of content encrypting data.
- Subsequent values of an increasing counter are added to a nonce value and the results are encrypted as usual.
- The nonce plays same role as initialization vectors in previous modes.
- If one bit of a plaintext or ciphertext message is damaged, only one corresponding output bit is damaged as well. Thus, it is possible to use various correction algorithms to restore the previous value of damaged parts of received messages.

CTR Encryption



CTR Decryption



Standards

Standard	Description
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 (HMAC)
PKCS #1	RSA Cryptography Standard
PKCS #3	Diffie-Hellman Key Agreement Standard
PKCS #5	Password-based Encryption Standard
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)
RFC 2104	Hash-based Message Authentication (HMAC)
RFC 3174	Secure Hash Algorithm (SHA-1)
RFC 2040	Block Padding
PKCS #7	Block Padding
NIST 800-38A	CBC (Cipher-Block Chaining) Cipher Mode

Historical

Year	Event
1466	Cipher disk invented by Leon Alberti
1553	Vigenere Cipher invented by Giovan Battista Bellaso
1854	Playfair Cipher invented by Charles Wheatstone
1863	First successful attack on the Vigenere Cipher published by Friedrick Kasiski
1918	ADFGVX Cipher invented by Colonel Fritz Nebel
1918	Enigma Machine invented by Arthur Scherbius
WW2	Enigma Machine used by Nazi Germany
1977	RSA invented by Ron Rivest, Adi Shamir, and Len Aldeman
1988	X.509 first used
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 with FIPS 197

Cipher	Description
Mono-Alphabet Substitution Cipher	Single alphabet
Atbash	Reverses the alphabet (A becomes Z, B becomes Y ...)
Caesar	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 Cipher	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.
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.
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.

Playfair Cipher	Invented by Charles Wheatstone in 1854. Uses a 5x5 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'.)
	`P L A Y F`
	`I R E X M`
	`B C D G H`
	`K N O Q S`
	`T U V W Z`

<table>
<tr><th>Cipher</th><th>Description</th></tr>
<tr><td>ADFGVX Cipher</td><td>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.
<table>
<tr><th></th><th>A</th><th>D</th><th>F</th><th>G</th><th>X</th></tr>
<tr><td>A</td><td>M</td><td>O</td><td>N</td><td>K</td><td>E</td></tr>
<tr><td>D</td><td>Y</td><td>S</td><td>A</td><td>B</td><td>C</td></tr>
<tr><td>F</td><td>D</td><td>F</td><td>G</td><td>H</td><td>I</td></tr>
<tr><td>G</td><td>L</td><td>P</td><td>Q</td><td>R</td><td>T</td></tr>
<tr><td>X</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr>
</table></td></tr>
<tr><td>The Enigma Machine</td><td>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.</td></tr>
<tr><td>Affine Cipher</td><td>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.</td></tr>
</table>

Hashes, Key Exchange, & Misc.

Key Exchange Algorithms
Diffie-Hellman (DH)
Menezes-Qu-Vanstone (MQV)
Key Exchange Algorithm (KEA)
Elliptic Curve Diffie-Hellman (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	SHA-2 (SHA256-SHA384) *(Message Digest)*

Secure Channel	Notes
OCB (Offset Codebook Mode)	Fast, but patent issues.
CCM (Counter with CBC-MAC Mode)	Slower than OCB but no known patent issues.
CWC (Carter-Wegman CTR Mode)	Speed improvement on CCM. No known patent issues.
GCM (Galois Counter Mode)	NIST standard block cipher mode. Improvement on CWC. No known patent issues.

Hash Function	Description
MD5	128-bit hash RFC 1321
MD6	Submitted to the NIST SHA-3 Competition
SHA	160-bit hash SHA-1 SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512) SHA-3
FORK 256	Uses 512-bit blocks 256-bit hash
RIPEMD-160	160-bit hash 128, 256, 320 versions exist
GOST	Defined by Russian National Standard 256-bit output
TIGER	192-bit hash
MAC & HMAC	A MAC uses a block cipher in CBC mode to improve integrity

WiFi Encryption	Notes
WEP (Wired Equivalent Privacy)	RC4 128-bit or 256-bit to secure data and CRC-32 for checksum
WPA	PSK (Pre-shared Key & TKIP)
WPA2	802.1x Introduces CCMP (Counter mode with Cipher Block Chaining)

Definitions

Term	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	plaintext
C	cyphertext
I(P)	length of plaintext in bytes
b	block size
K	number of blocks
K_o	key stream
$\oplus$	XOR
M	blocks in total
n	block size of block cipher
h	iterative hash function
T	tag

Random Number Generators

Random Number Generator Types
Table Lookup Generators
Hardware Generators
Algorithmic (Software) Generators

Algorithmic Pseudo Random Number Generator	Description
Linear Congruential Generators	The algorithm is: Xn+1=(aXn+c) Mod m where n>0
Lagged Fibonacci Generator (LFG)	formula: y= Xk+Xj+1. can be Additive LFG, Multiplicative LFG or Two-tap LFG
Blum Blum Shub	The algorithm is: Xn+1=Xn2 Mod 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.

Formulas

Name	Notes	Formula
RSA	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)