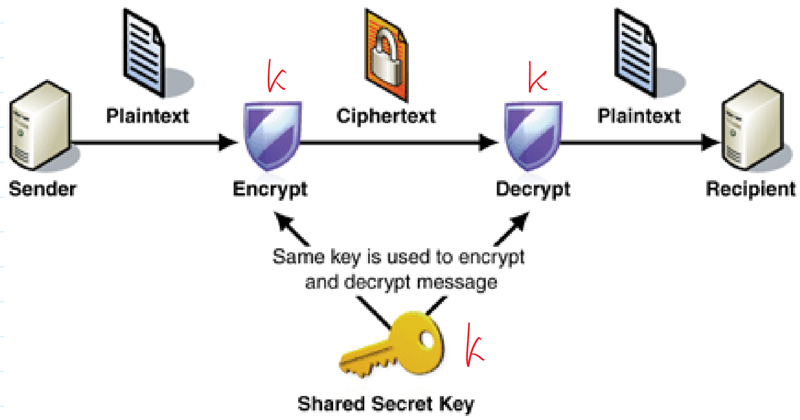


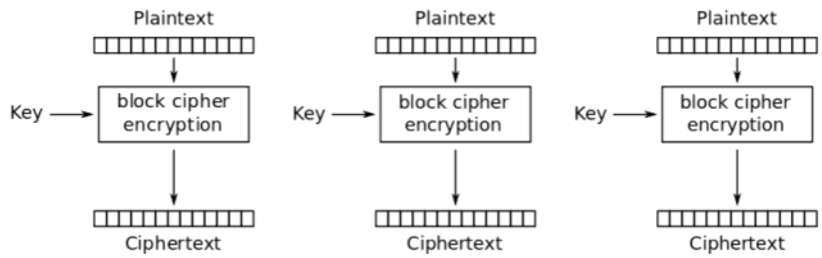
In cryptography, a **block cipher mode of operation** is an algorithm that uses a block cipher to provide information security such as confidentiality or authenticity.
A block cipher by itself is only suitable for the secure cryptographic transformation (encryption or decryption) of one fixed-length group of bits called a block.
A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block.

Most modes require a unique binary sequence, often called an initialization vector (**IV**), for each encryption operation. The **IV** has to be non-repeating and, for some modes, random as well.
The initialization vector is used to ensure distinct ciphertexts are produced even when the same plaintext is encrypted multiple times independently with the same key.
Block ciphers may be capable of operating on more than one block size, but during transformation the block size is always fixed. 128, 192, 256
Block cipher modes operate on whole blocks and require that the last part of the data be padded to a full block if it is smaller than the current block size.

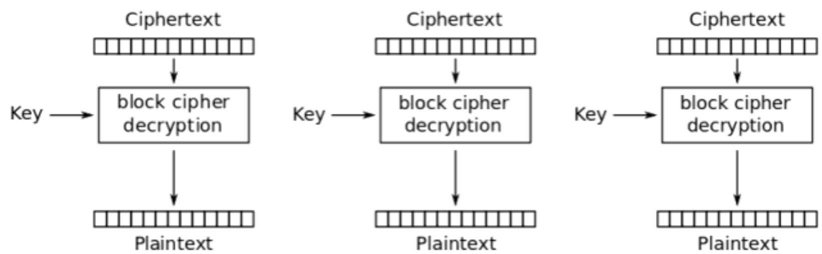
An initialization vector has different security requirements than a **key**, so the **IV** usually does not need to be secret.
However, in most cases, it is important that an **IV** is never reused under the same key.
For CBC and CFB, reusing an **IV** leaks some information about the first block of plaintext, and about any common prefix shared by the two messages.
For OFB and CTR, reusing an **IV** completely destroys security.
This can be seen because both modes effectively create a bitstream that is **XORed** with the plaintext, and this bitstream is dependent on the key and **IV** only.
Reusing a bitstream destroys security.
In CBC mode, the **IV** must, in addition, be **unpredictable at encryption time**; in particular, the (previously) common practice of re-using the last ciphertext block of a message as the **IV** for the next message is insecure (for example, this method was used by SSL 2.0).
If an attacker knows the **IV** (or the previous block of ciphertext) before the next plaintext is specified, they can check their guess about plaintext of some block that was encrypted with the same key before (this is known as the TLS CBC **IV** attack).

Electronic codebook (ECB)

The simplest of the encryption modes is the **electronic codebook** (ECB) mode (named after conventional physical codebooks). The message is divided into blocks, and each block is encrypted separately



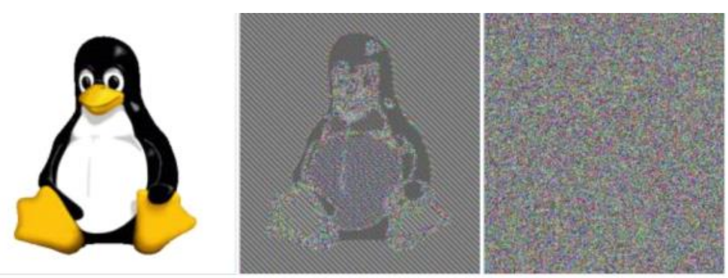
Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

(a) plaintext

(b) plaintext encrypted in ECB mode using AES



Original image

Encrypted using ECB mode

Modes other than ECB result in pseudo-randomness

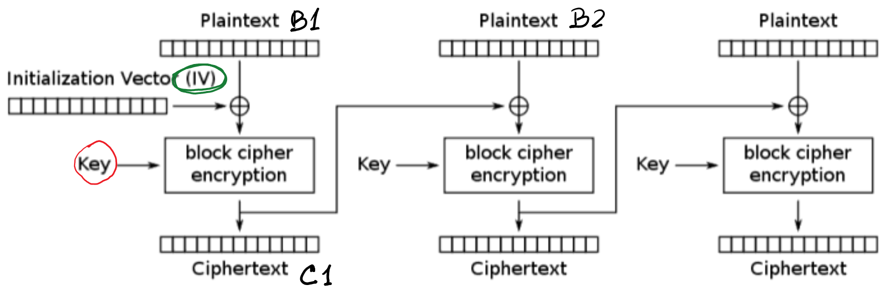
Cipher block chaining (CBC)

Ehrsam, Meyer, Smith and Tuchman invented the cipher block chaining (CBC) mode of operation in 1976.

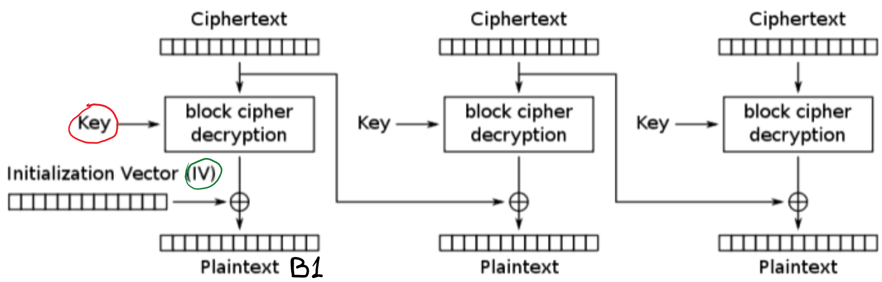
In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted.

This way, each ciphertext block depends on all plaintext blocks processed up to that point.

To make each message unique, an initialization vector - **IV** must be used in the first block.



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

CBC	
Cipher block chaining	
Encryption parallelizable:	No
Decryption parallelizable:	Yes
Random read access:	Yes

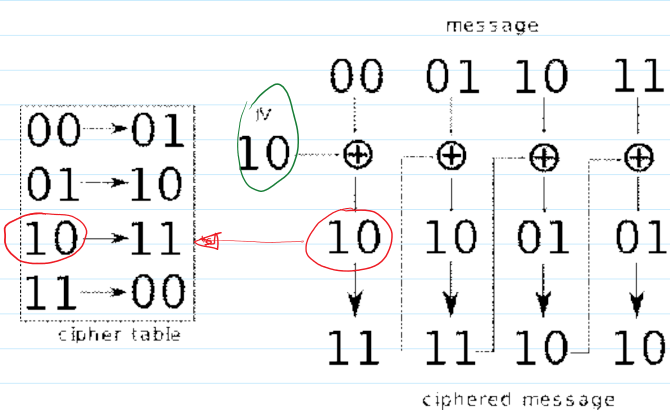
If the first block has index 1, the mathematical formula for CBC encryption is

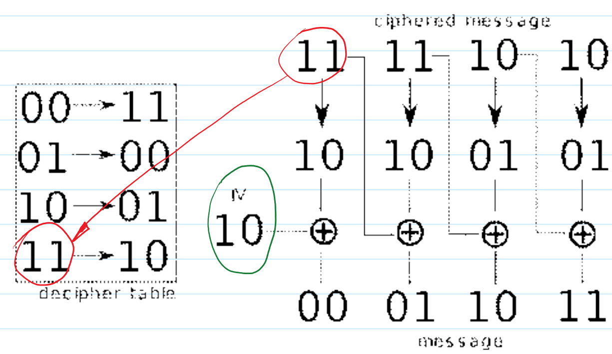
$$C_i = E_K(P_i \oplus C_{i-1}),$$
$$C_0 = IV,$$

The mathematical formula for CBC decryption is:

$$P_i = D_K(C_i) \oplus C_{i-1},$$
$$C_0 = IV.$$

Example





CBC has been the most commonly used mode of operation. Its main drawbacks are that encryption is sequential i.e., it cannot be parallelized.

CBC H   CBCHMAC

Counter (CTR)

CTR mode like OFB, counter mode turns a block cipher into a stream cipher.   NSA

It generates the next keystream block by encrypting successive values of a "**C**oun**T**e**R**". The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual increment-by-one counter is the simplest and most popular.

The usage of a simple deterministic input function used to be controversial; critics argued that "deliberately exposing a cryptosystem to a known systematic input represents an unnecessary risk." However, today CTR mode is widely accepted and any problems are considered a weakness of the underlying block cipher, e.g. **AES** which is expected to be secure regardless of systemic bias in its input.

Along with CBC, CTR mode is one of two block cipher modes recommended by Niels Ferguson and Bruce Schneier.

CTR mode was introduced by Whitfield Diffie and Martin Hellman in 1979.

CTR mode has similar characteristics to OFB, but also allows a random access property during decryption.

CTR mode is well suited to operate on a multi-processor machine where blocks can be encrypted in parallel.

Furthermore, it does not suffer from the short-cycle problem that can affect OFB.

If the **IV/nonce** is random, then they can be combined together with the counter using any invertible operation (concatenation, addition, or XOR) to produce the actual unique counter block for encryption.

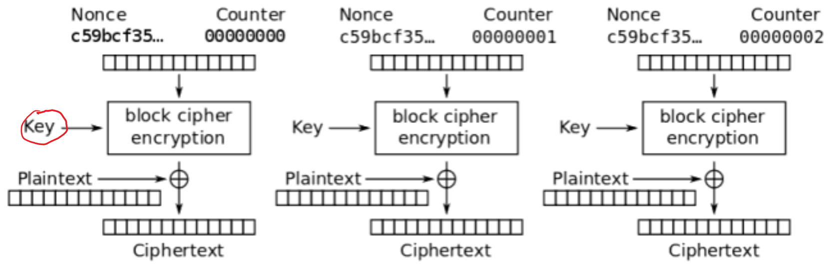
In case of a non-random nonce (such as a packet counter), the nonce and counter should be concatenated (e.g., storing the nonce in the upper 64 bits and the counter in the lower 64 bits of a 128-bit counter block).

Simply adding or XORing the nonce and counter into a single value would break the security under a chosen-plaintext attack in many cases, since the attacker may be able to manipulate the entire IV–counter pair to cause a collision.

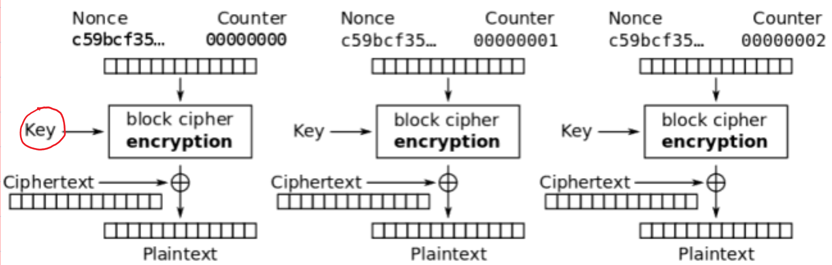
Once an attacker controls the IV–counter pair and plaintext, XOR of the ciphertext with the known plaintext would yield a value that, when XORed with the ciphertext of the other block sharing the same IV–counter pair, would decrypt that block.

Note that the nonce in this diagram is equivalent to the initialization vector (IV) in the other diagrams.

However, if the offset/location information is corrupt, it will be impossible to partially recover such data due to the dependence on byte offset.



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Counter CTR	
Encryption parallelizable:	Yes
Decryption parallelizable:	Yes
Random read access:	Yes

$a = g^x \bmod p$

Cryptographic hash functions

$2^{256} \to 2^{255}$

A **cryptographic hash function** is a special class of hash function that has certain properties which make it suitable for use in cryptography. It is a mathematical algorithm that maps data of finite size to a bit string of a fixed size (a hash function) which is designed to also be a one-way function, that is, a function which is infeasible to invert.
The only way to recreate the input data from an ideal cryptographic hash function's output is to attempt a brute-force search of possible inputs to see if they produce a match.
The input data is often called the *message*, and the output (the *hash value* or *hash*) is often called the *message digest* or simply the *digest*.

From <https://en.wikipedia.org/wiki/Cryptographic_hash_function>

m – message (finite length)

$h = H(m)$

$|h| = 256$ bits

$|h| = 28$ bits $= 7$ hex numb.

$0000_b = 0_h \equiv 0_d$

$0001_b = 1_h \equiv 1_d$

$0010_b = 2_h \equiv 2_d$

$1001 = 9_{16} \equiv 9_{10}$

$1010 = A_{16} \equiv 10_{10}$

$1110 = E_h \equiv 14_{10}$

$1111 = F_h = 15_{10}$

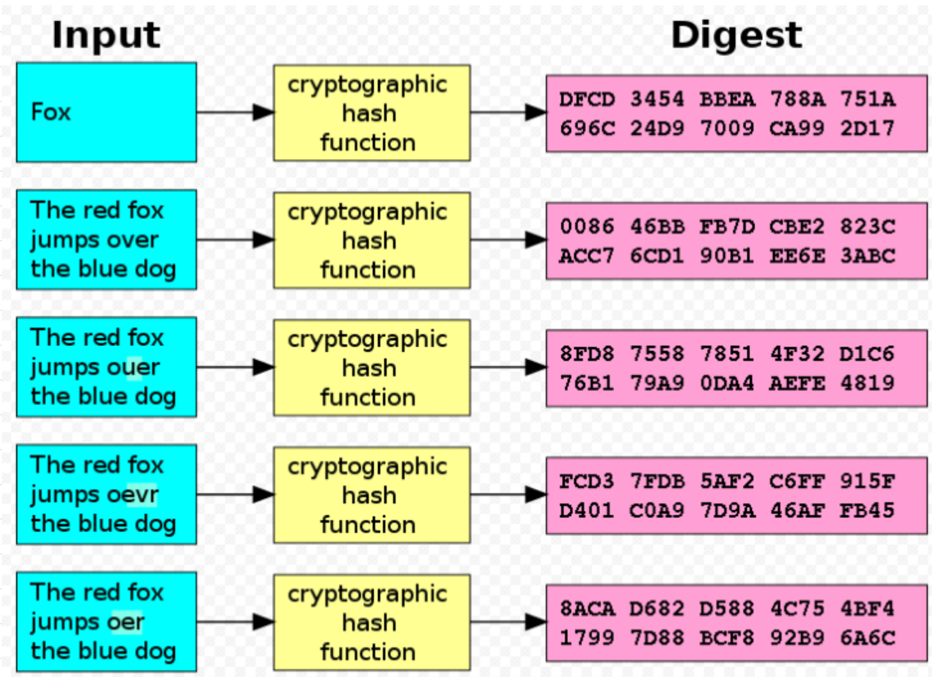
1) When given m and H( ), then it is easy to compute $h = H(m)$.

2) It is infeasible to find any m' such that $H(m') = h$.

2) It is infeasible to find any m such that $H(m') = h$.

$1110 = E_h = 14_{10}$
$1111 = F_h = 15_{10}$

Cryptographic hash functions have many information-security applications, notably in digital signatures, message authentication codes (HMACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information-security contexts, cryptographic hash values are sometimes called (*digital*) *fingerprints*, *checksums*, or just *hash values*, even though all these terms stand for more general functions with rather different properties and purposes.



SHA-1

40 Hex numbers = 160 bits

SHA-1

$SHA\text{-}1: \{0,1\}^* \to \{0,1\}^{160}$

Avelange effect

A cryptographic hash function (specifically SHA-1) at work. A small change in the input (in the word "over") drastically changes the output (digest). This is the so-called avalanche effect.

Properties

- it is quick to compute the hash value for any given message.
- a small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value.

Most cryptographic hash functions are designed to take a string of any finite length as input and produce a fixed-length hash value.
A cryptographic hash function must be able to withstand all known types

of cryptanalytic attack.

In theoretical cryptography, the security level of a cryptographic hash function has been defined using the following properties:

- ***Pre-image resistance***
  Given a hash value ***h*** it should be difficult to find any message ***m'*** such that ***h* = *hash(m')***. This concept is related to that of one-way function. Functions that lack this property are vulnerable to preimage attacks.

- ***Second pre-image resistance***
  Given an input m_1 it should be difficult to find (different) input m_2 such that $hash(m_1) = hash(m_2)$.
  Functions that lack this property are vulnerable to second-preimage attacks.

- ***Collision resistance***
  It should be difficult to find any two different messages m_1 and m_2 such that $hash(m_1) = hash(m_2)$. Such a pair is called a cryptographic hash collision. This property is sometimes referred to as *strong collision resistance.* It requires a hash value at least twice as long as that required for preimage-resistance; otherwise **collisions** may be found by a birthday attack.[2]

These properties form a hierarchy, in that collision resistance implies second pre-image resistance, which in turns implies pre-image resistance, while the converse is not true in general. [3]

The weaker assumption is always preferred in theoretical cryptography, but in practice, a hash-functions which is only second pre-image resistant is considered insecure and is therefore not recommended for real applications.

Informally, these properties mean that a malicious adversary cannot replace or modify the input data without changing its digest.

Thus, if two strings have the same digest, one can be very confident that they are identical.

m_1 – loan contract

$H(m_1) = h_1$

$Sig(h_1) = S_1$

$m_2 = 100\,000$ €

$H(m_1) = H(m_2)$

SHA-256

64 Hex digits

sha256('....')

Illustration

nonce = 737327631

```
>> sha256('RootHash PrevHash 737327631')
ans = F4AE534CD226FAF799  8C8424B348E020BA80639A687E93A0B8C5130ED  C51E6DE
>> sha256('RootHash PrevHash 737327632')
ans = B856211DF2EE15E30AB770C1A43CE014ECFE573182AFD885B28D96854DBC5F21
>> sha256('RootHash PrevHash 737327633')
ans = 9C18C764E347A58E57AC3F7A3C2874D5889A0E802699FEA47EEFF8C03BFEDA69
```

h28('....')

$0_h \equiv 0000_2$; $F_h \equiv 1111_2$

h28('....') → 7 hex numb.

h28('....') → decimal num.

hd28('...') → decimal num.

Commitment

An illustration of the potential use of a cryptographic hash is as follows: Alice poses a tough math problem to Bob and claims she has solved it. Bob would like to try it himself, but would yet like to be sure that Alice is not bluffing.

$P = NP$

$P \neq NP$

Therefore, Alice writes down her solution, computes its hash and tells Bob the hash value (whilst keeping the solution secret).

Then, when Bob comes up with the solution himself a few days later, Alice can prove that she had the solution earlier by revealing it and having Bob hash it and check that it matches the hash value given to him before. (This is an example of a simple commitment scheme; in actual practice, Alice and Bob will often be computer programs, and the secret would be something less easily spoofed than a claimed puzzle solution).

Verifying the integrity of files or messages

Main article: File verification

An important application of secure hashes is verification of message integrity. Determining whether any changes have been made to a message (or a file), for example, can be accomplished by comparing message digests calculated before, and after, transmission (or any other event).

$f \neq f'$

$H(f) \neq H(f')$

For this reason, most digital signature algorithms only confirm the authenticity of a hashed digest of the message to be "signed". Verifying the authenticity of a hashed digest of the message is considered proof that the message itself is authentic.

MD5, SHA1, or SHA2 hashes are sometimes posted along with files on websites or forums to allow verification of integrity.[6] This practice establishes a chain of trust so long as the hashes are posted on a site authenticated by HTTPS.

Password verification[edit]

Main article: password hashing

A related application is password verification (first invented by Roger Needham). Storing all user passwords as cleartext can result in a massive security breach if the password file is compromised. One way to reduce this danger is to only store the hash digest of each password. To authenticate a user, the password presented by the user is hashed and compared with the stored hash. (Note that this approach prevents the original passwords from being retrieved if forgotten or lost, and they have to be replaced with new ones.) The password is often concatenated with a random, non-secret salt value before the hash function is applied. The salt is stored with the password hash. Because users have different salts, it is not feasible to store tables of precomputed hash values for common passwords. Key stretching functions, such as PBKDF2, Bcrypt or Scrypt, typically use repeated invocations of a cryptographic hash to increase the time required to

nonce

perform brute force attacks on stored password digests.
In 2013 a long-term Password Hashing Competition was announced to choose a new, standard algorithm for password hashing.

Proof-of-work

Main article: Proof-of-work system

A proof-of-work system (or protocol, or function) is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer. A key feature of these schemes is their asymmetry: the work must be moderately hard (but feasible) on the requester side but easy to check for the service provider. One popular system — used in Bitcoin mining and Hashcash — **uses partial hash inversions to prove that work was done,** as a good-will token to send an e-mail. The sender is required to find a message whose hash value begins with a number of zero bits. The average work that sender needs to perform in order to find a valid message is exponential in the number of zero bits required in the hash value, while the recipient can verify the validity of the message by executing a single hash function. For instance, in Hashcash, a sender is asked to generate a header whose 160 bit SHA-1 hash value has the first 20 bits as zeros. The sender will *on average* have to try 2^{19} times to find a valid header.

$2^{20} = 1M$

File or data identifier

A message digest can also serve as a means of reliably identifying a file; several source code management systems, including Git, Mercurial and Monotone, use the sha1sum of various types of content (file content, directory trees, ancestry information, etc.) to uniquely identify them. Hashes are used to identify files on peer-to-peer filesharing networks.

Pseudorandom generation and key derivation

Hash functions can also be used in the generation of pseudorandom bits, or to derive new keys or passwords from a single secure key or password.

As of 2009, the two most commonly used cryptographic hash functions were MD5 and SHA-1. However, a successful attack on MD5 broke Transport Layer Security in 2008.

$1K = 2^{10} = 1024$
$1M = 2^{20}$
$1G = 2^{30}$
$1T = 2^{40}$
2^{112}

In February 2005, an attack on SHA-1 was reported that would find collision in about 2^{69} hashing operations, rather than the 2^{80} expected for a 160-bit hash function. In August 2005, another attack on SHA-1 was reported that would find collisions in 2^{63} operations. Though theoretical weaknesses of SHA-1 exist,[14][15] no collision (or near-collision) has yet been found. Nonetheless, it is often suggested that it may be practical to break within years, and that new applications can avoid these problems by using later members of the SHA family, such as SHA-2.

SHA-2 (**Secure Hash Algorithm 2**) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA).[3]

From <https://en.wikipedia.org/wiki/SHA-2>

SHA-2 includes significant changes from its predecessor, SHA-1.
The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits:
SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.

h28

However, to ensure the long-term robustness of applications that use hash functions, there was a competition to design a replacement for SHA-2.
On October 2, 2012, Keccak was selected as the winner of the NIST hash function competition.
A version of this algorithm became a FIPS standard on August 5, 2015 under the name SHA-3.

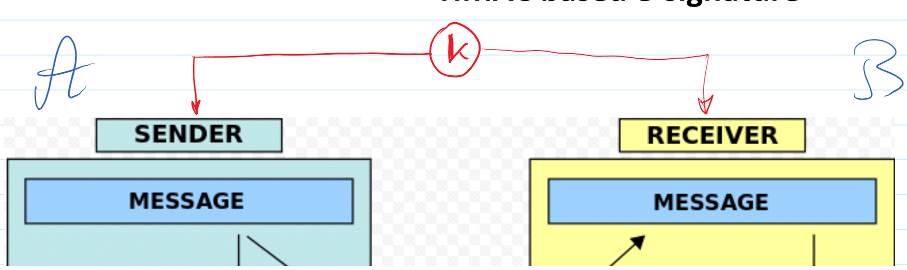
HMAC

Use in building other cryptographic primitives
Hash functions can be used to build other cryptographic primitives.
For these other primitives to be cryptographically secure, care must be taken to build them correctly.
Message authentication codes (MACs) (also called keyed hash functions) are often built from hash functions. HMAC is such a MAC.

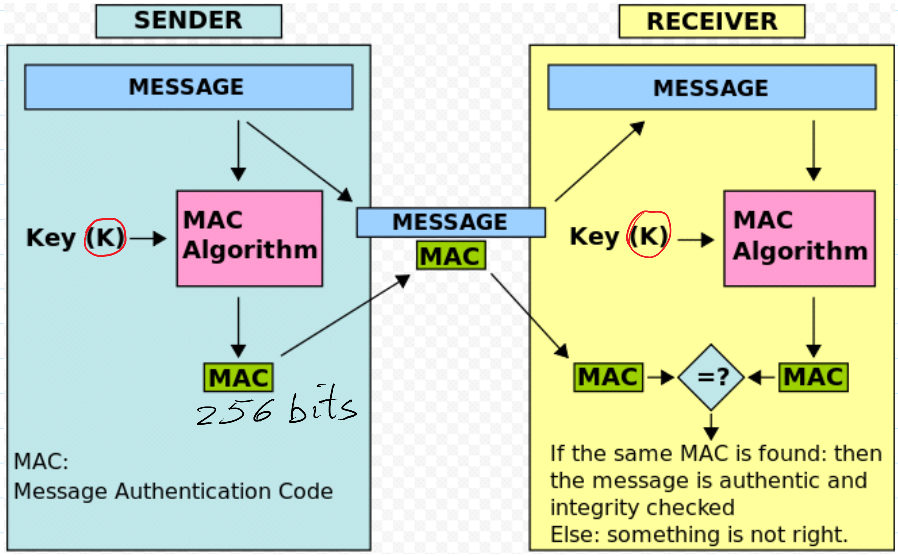
Information
Authentication
Integrity

Keyed-hash message authentication code (**HMAC**) is a specific type of message authentication code (MAC) involving a cryptographic hash function (hence the 'H') in combination with a secret cryptographic key.
As with any MAC, it may be used to *simultaneously* verify both the *data integrity* and the *authentication* of a message.
Any cryptographic hash function, may be used in the calculation of an HMAC.
The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key.

HMAC based e-signature



Authentic
Integral



Authentic
Integral

Įdiegti šiuos .m failus į Octave, išzipuojant failą iš http://crypto.fmf.ktu.lt/xdownload/

h26	2020.03.22 17:08
H26d	2019.10.26 14:30
h28	2020.03.22 17:08
H28d	2019.10.23 22:42
hd26	2020.03.22 17:08
hd28	2020.03.22 17:08

- Octave_Stud 2020.03.22.7z

Till this place

Hash functions based on block ciphers

There are several methods to use a block cipher to build a cryptographic hash function, specifically a one-way compression function.
The methods resemble the block cipher modes of operation usually used for encryption.
Many well-known hash functions, including MD4, MD5, SHA-1 and SHA-2 are built from block-cipher-like components

HMAC can be constructed form the block cipher using cipher block chaining (CBC) mode of operation.

AES_K-CBC

CBC-MAC

M – to be signed.

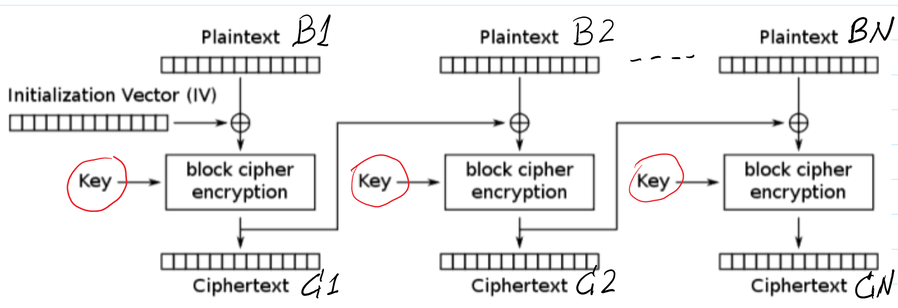
CBC-MAC

M – to be signed.

$C = AES\_CBC(k, M)$

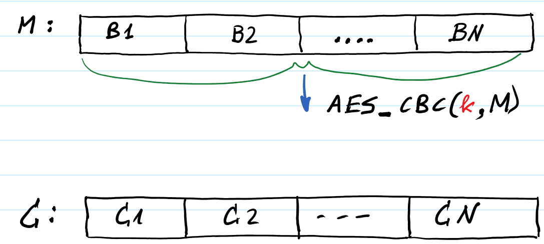
Cipher block chaining message authentication code (**CBC-MAC**) is a technique for constructing a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode to create a chain of blocks such that each block depends on the proper encryption of the previous block. This interdependence ensures that a change to any of the plaintext bits will cause the final encrypted block to change in a way that cannot be predicted or counteracted without knowing the key to the block cipher.

From <https://en.wikipedia.org/wiki/CBC-MAC>



Cipher Block Chaining (CBC) mode encryption

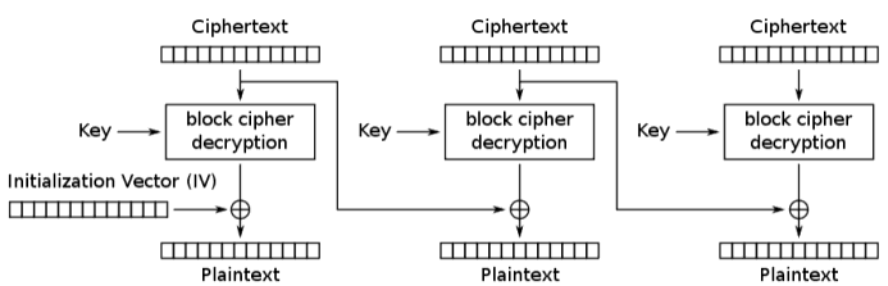
$|k| = 256\,b \Rightarrow |B_i| = |C_i| = 256$



$HMAC = C_1 \oplus C_2 \oplus \ldots \oplus C_N = h$

bitwice XORing

$|h| = 256\,b.$



Cipher Block Chaining (CBC) mode decryption

Asymmetric Signing - Verification

Public Parameters - PP: >> **p** = 264043379; >> **g**=2;

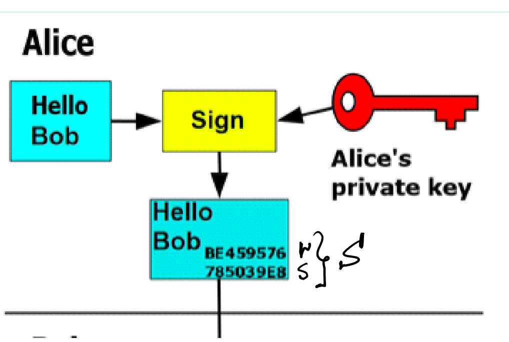
>> p = 251487959; >> g=7; Changed!

$Z_p^* = \{1, 2, \ldots, p-1\}$

Signature Creation - Verification

S=Sig(PrK$_A$, h)

V=Ver(PuK$_A$, S, h), V∈{True, False}≡{1, 0}



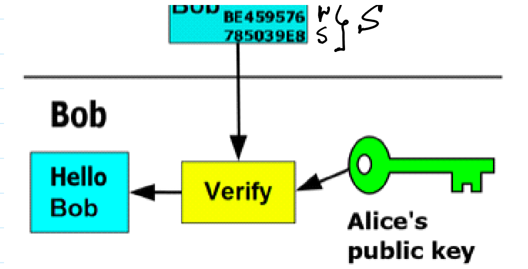
Signature creation by Alice:

M - any message of finite length to be signed.

1. **M is hashed with h-function H() by computing its h-value h=H(M)**
2. **Signature is computed on h-value h: S=Sig(PrK$_A$, h)=(r,s).**

Signature verification:

1. **Received message M' is hashed by receiver Bob h'=H(M').**
2. **Signatutre is verified by verification**



IBM Hyperledger Fabric
IBM Trust Food

Bob **h'=H(M').**

2. **Signatutre is verified by verification function Ver(PuK_A, S, h').**

If PrK_A=x, PuK_A=a and $a = g^x \bmod p$

AND

If M=M'

Then signature is valid and V∈{True}.

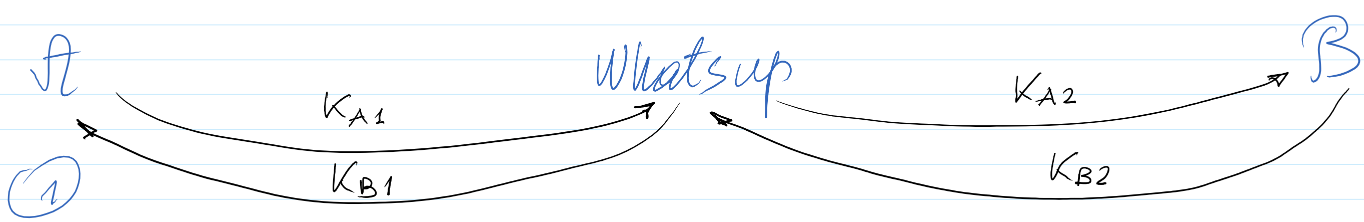
********************************** Till this place ****************

M - message to be hashed

k - secret encr. key

A(k) B(k)

A: wish to encr. message m together wit providing its authenticity and integrity.



$$K_{AB} = \underbrace{(K_B)^x \bmod p}_{K_1} = K = \underbrace{(K_A)^y \bmod p}_{K_2} = K_{BA}$$

m - message

$Enc(K_1, m) = C_1$ ⟶ $Dec(K_1, C_1) = m$

$Dec(K_1, C_1) = m$

↓

Data center

$Enc(K_2, m) = C_2$ ⟶ $Dec(K_2, C_2) = m$

(2) Whatsup software and its updating

Whatsup ↓ Backdoors ⟶ updating

Chosen Plaintext Attack

A:

$E_{CBC}(k, m) = c$
$H_{CBC}(k, c) = h$
} encrypt & hash

c, h ⟶

B:
1) $H_{CBC}(k, c) = h'$

? $h \stackrel{?}{=} h'$ if ok

2) $D(k, c) = m$