

Gerb. Studentai.

Modulio P170M100 koliokviumas **Informatikams** vyks Lapkričio 7 d., 18:30, per Zoom:

<https://liedm.zoom.us/j/9999112448>

Passcode: 12345678

Per koliokviumą Jūs turėsite išspręsti 2 užduotis iš:

<https://imimsociety.net/en/>

Registracija į <https://imimsociety.net/en/> galima be skaičių, todėl pvz. **Jonas Petraitis** registruojasi taip:

[Name] **Jonas** [Surname] **Pe**

Visi kiti registracijos duomenys išskyrus e-paštą gali būti bet kokie.

Prisiregistravę Jūs gausite 10 Eur virtualių pinigų, už kuriuos galite pirkti reikalingas išspręsti 2 užduotis.

**Dėmesio:** pirkite tiktai po vieną užduotį ir ją išsprendus pirkite kitą.

Prieš koliokviumą galite treniruotis ir spręsti užduotis kiek norite kartų.

Jei nesėkmingai išėikvojote visus pinigus, prisiregistruokite kitu vardu, pvz. **Pee**.

1-užduotis:

<https://imimsociety.net/en/cryptography/29-diffie-hellman-key-agreement-protocol.html>

2- užduotis:

<https://imimsociety.net/en/cryptography/32-man-in-the-middle-attack.html>

Jeigu sprendimas teisingas, Jums reikia paspausti mygtuką [**Get Reward**], tik tada uždavinys yra įskaitytas ir užregistruotas duomenų bazėje, o Jūs gaunate atlyginimą dvigubai tiek, kiek sumokėjote virtualių pinigų. Pasitikrinti galite dešinėje viršuje paspaudę savo registracijos mygtuką.

Jei sprendimas neteisingas, paspauskite viršuje kairėje esantį mygtuką [Return].

Kad geriau susipažintumėte su sprendimo procesu, aš rekomenduoju Jums išspręsti Vilko, Ožkos ir Kopūsto perkėlimo per upę intelektualinį uždavinį iš skyriaus:

<https://imimsociety.net/en/16-intellect>

[YYMMDD]

[020523]

[23051997]

[137256121]

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 arbitrary 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](https://en.wikipedia.org/wiki/Cryptographic_hash_function)

$M$  - <sup>finite length</sup> message

$$h = H(M)$$

$$|h| = 256 \text{ bits}$$

$$|h| = 28 \text{ bits}$$

$$= 7 \text{ hex numb.}$$

$$0000_b = 0_h \equiv 0_d$$

$$0001_b = 1_h \equiv 1_d$$

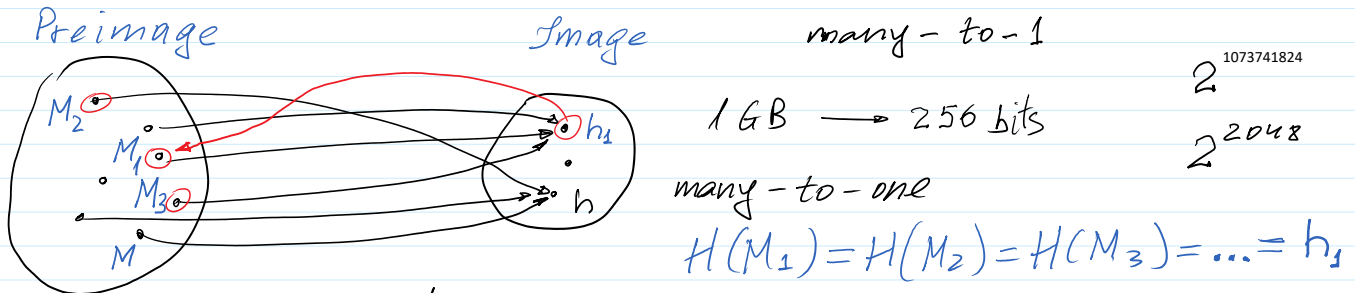
$$0010_b = 2_h \equiv 2_d$$

$$\bar{1}\bar{0}\bar{0}\bar{1}_b = 9_h \equiv 9_{10}$$

$$\begin{aligned} \overline{1001}_b &= 9_h = 9_{10} \\ 1010_b &= A_h = 10_{10} \\ \underline{1011}_b &= B_h = 11_{10} \\ 1110_b &= E_h = 14_{10} \\ 1111_b &= F_h = 15_{10} \end{aligned}$$

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*, *message digest* or just *hash values*, even though all these terms stand for more general functions with rather different properties and purposes.

$M$  - message ;  $H(M) = h$   
 $M \in \{0,1\}^*$  ;  $h \in \{0,1\}^{256}$  ;  $H: \{0,1\}^* \rightarrow \{0,1\}^{256} // \text{SHA256}$

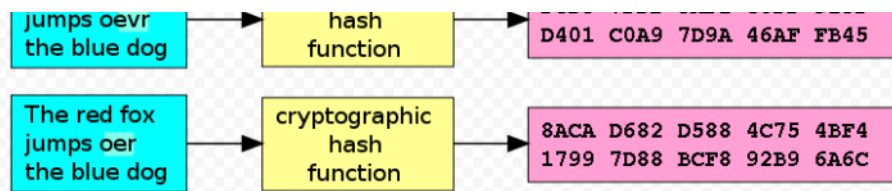


For given  $h_1$  it is infeasible to find any  $M_i$  satisfying:  
 $H(M_i) = h_1$

| Input                               | cryptographic hash function | Digest   |
|-------------------------------------|-----------------------------|--|
| Fox                                 | cryptographic hash function | DFCD 3454 BBEA 788A 751A<br>696C 24D9 7009 CA99 2D17 |
| The red fox jumps over the blue dog | cryptographic hash function | 0086 46BB FB7D CBE2 823C<br>ACC7 6CD1 90B1 EE6E 3ABC |
| The red fox jumps over the blue dog | cryptographic hash function | 8FD8 7558 7851 4F32 D1C6<br>76B1 79A9 0DA4 AEF6 4819 |
| The red fox jumps over the blue dog | cryptographic hash function | FCD3 7FDB 5AF2 C6FF 915F<br>D401 C0A9 7D9A 46AF FB45 |

40 Hex numbers = 160 bits

SHA-1  
 $SHA-1: \{0,1\}^* \rightarrow \{0,1\}^{160}$   
 $2^{160}$   
 Lavinos efektas  
 Avalanche effect  
 $\sim 160$  bitolans  $\sim 80$



rikkunngj eptevv  
 $2^{160}$  Birthday  $\rightarrow$   $2^{80}$   
 Pat.

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 finite 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.
- Security properties presented below.

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  $h = H(M)$ . This concept is related to that of [one-way function](#). Functions that lack this property are vulnerable to [first preimage attacks](#).

- **Second pre-image resistance**

Given an input  $M_1$  it should be difficult to find (different) input  $M_2$  such that  $H(M_1) = H(M_2)$ . Functions that lack this property are vulnerable to [second-preimage attacks](#).

- **Collision resistance**

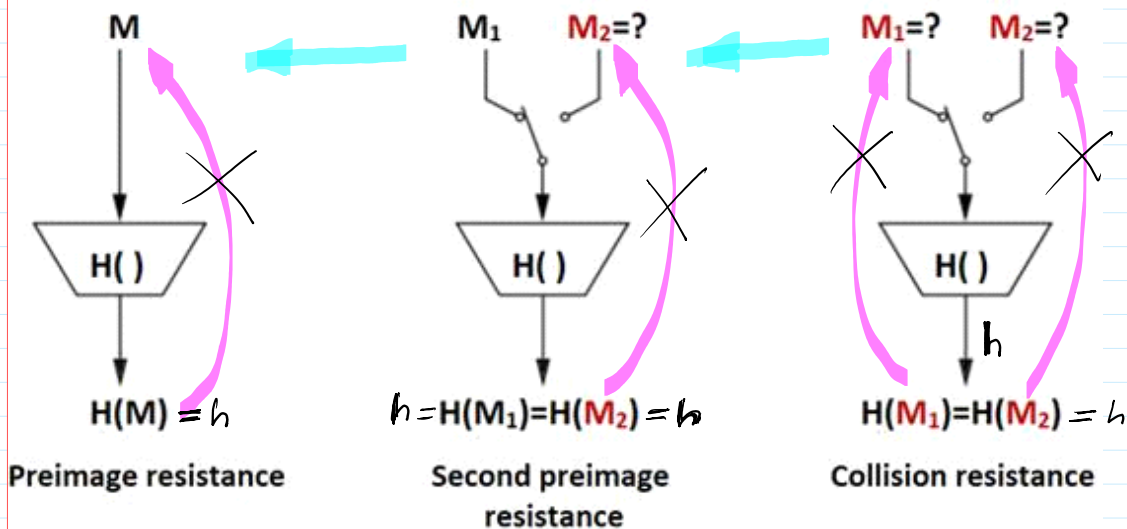
It should be difficult to find any two different messages  $M_1$  and  $M_2$  such that  $H(M_1) = H(M_2)$ . Such a pair is called a cryptographic [hash collision](#). This property is sometimes referred to as **strong collision resistance**. It requires a hash value at least twice as long as that required for preimage-resistance; otherwise **collisions** may be found by a [birthday attack](#).<sup>[2]</sup>

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. <sup>[3]</sup>

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.



### Loan contract

$M_1 = 1000 \text{€ loan.}$

$M_1$  - is a valid loan contract.

$h = H(M_1); |h| = 256 \text{ bits}$

Alice:  $PrK_A = x \rightarrow \text{Sign}(PrK_A, h) = \sigma_h = (r_A, s_A)$

$PuK_A = a$

$M_1, \sigma_h, PuK_A$

Joe: finds second preimage  $M_2$  to create loan contract for 100000€ such that  $H(M_1) = H(M_2) = h$

Then the valid signature on  $M_1$  is valid also on  $M_2$ .

Alice:  $h = H(M_2) \leftarrow M_2, \sigma_h$   
 Verif  $(\sigma_h, h, PuK_A) = \text{True}$

claim to Alice to pay 100000€ (instead of 1000€)

### Illustration

nonce = 737327631

```
>> sha256('RootHash PrevHash 737327631')
```

```
ans = F4AE534CD226FAF7998C8424B348E020BA80639A687E93A0B8C5130ED
```

$h_{28}(\dots)$   
 C51E6DE  
 C51E6DE

```
>> sha256('RootHash PrevHash 737327632')
```

```
ans = B856211DF2EE15E30AB770C1A43CE014ECFE573182AFD885B28D96854DBC5F21
```

```
>> sha256('RootHash PrevHash 737327633')
```

```
ans = 9C18C764E347A58E57AC3F7A3C2874D5889A0E802699FEA47EEFF8C03BFEDA69
```

$$O_h \equiv 0000_2 ; \quad F_h \equiv 1111_2$$

$h_{28}('...')$  → ≠ hex numb.  
 $hd_{28}('...')$  → 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).

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.<sup>[6]</sup> This practice establishes a [chain of trust](#) so long as the hashes are posted on a site authenticated by [HTTPS](#).

$$\begin{aligned} f &\neq f' \\ H(f) &\neq H(f') \\ h & \quad h' \\ \text{Sign}(PrK, h) &\neq \text{Sign}(PrK, h') \end{aligned}$$

## Password verification<sup>[edit]</sup>

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

Ethereum: keccak 256

passwords. [Key stretching](#) functions, such as [PBKDF2](#), [Bcrypt](#) or [Scrypt](#), typically use repeated invocations of a cryptographic hash to increase the time required to 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.

$$1K = 2^{10} = 1024$$

$$1M = 2^{20}$$

$$1G = 2^{30}$$

$$1T = 2^{40}$$

$$SHA1(M) = h$$

$$|h| = 160 \text{ bits}$$

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

operations. Though theoretical weaknesses of SHA-1 exist, 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](#).

$$\text{SHA1}(M) = h$$
$$|h| = 160 \text{ bits}$$

According to birthday paradox it is not required to scan all  $2^{160}$  variants of message  $M$ . It is enough to scan  $\sqrt{2^{160}} = 2^{80}$  variants.

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

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:

$h_{28}$

**SHA-224**, **SHA-256**, **SHA-384**, **SHA-512**, **SHA-512/224**, **SHA-512/256**.

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 - H Message Authentication Code

### 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

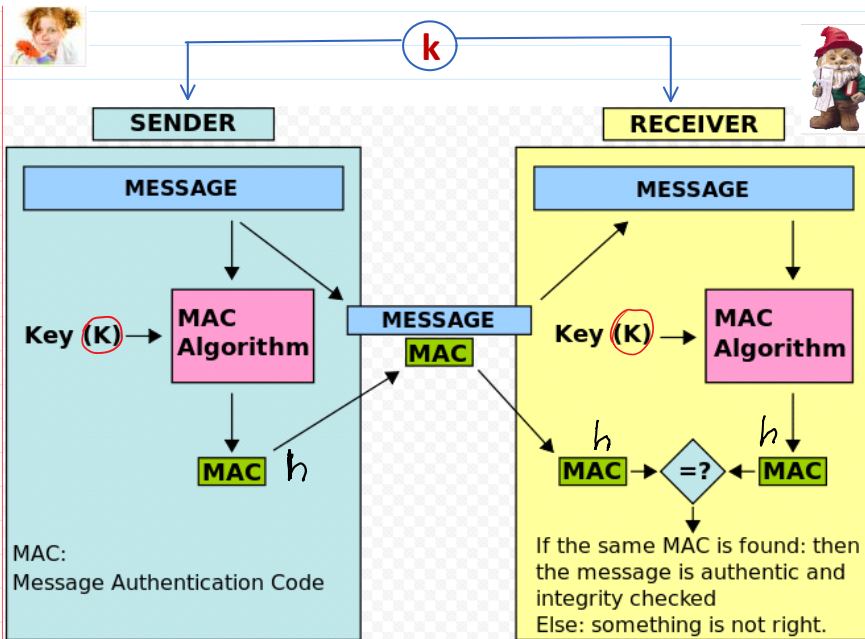
**Keyed-hash message authentication code (HMAC)** is a specific type of message authentication code (MAC) involving a cryptographic hash function (hence the 'H') in combination with a secret cryptographic key.

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*

Till this place

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 |
| <input checked="" type="checkbox"/> hd28 | 2020.03.22 17:08 |

• [Octave Stud 2020.03.22.7z](#)

```
>> sha256('RootHash PrevHash 737327631')
ans = F4AE534CD226FAF7998C8424B348E020BA80639A687E93A0B8C5130EDC51E6DE
>> h28('RootHash PrevHash 737327631')
ans = C51E6DE
>> hd28('RootHash PrevHash 737327631')
ans = 206694110
>> dec2bin(ans)
ans = 1100010100011110011011011110
>> dec2hex(206694110)
ans = C51E6DE
```

### 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 from the block cipher using cipher block chaining (CBC) mode of operation.

*AES<sub>k</sub>-CBC*

*M - to be signed.*

$$G = \text{AES\_CBC}(k, M)$$

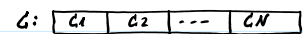
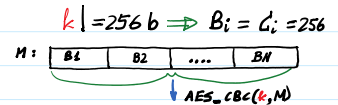
*↓  
256*

### CBC-MAC

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.

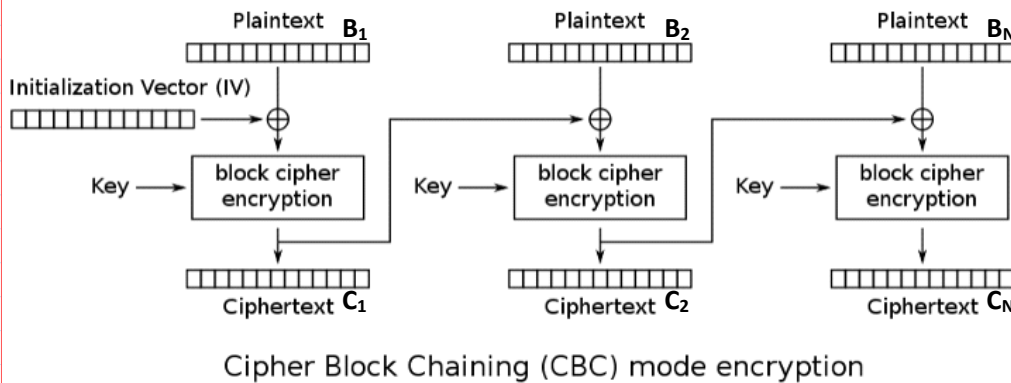
From <https://en.wikipedia.org/wiki/CBC-MAC>



$$h_{MAC} = C_1 \oplus C_2 \oplus \dots \oplus C_N = h$$

*bitwise XORing*

*|h| = 256 b.*



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

### Asymmetric Signing - Verification

Public Parameters - PP: >> p = 268 435 019; >> g=2;

$$\mathcal{I}_p^* = \{1, 2, \dots, p-1\}$$

### Signature Creation - Verification

$$S = \text{Sign}(\text{Pr}K_A, h) = \sigma = (r, s)$$

$$V = \text{Ver}(\text{Pu}K_A, \sigma, h) \quad V \in \{\text{True}, \text{False}\} = \{1, 0\}$$

### Signature creation by sender Alice:

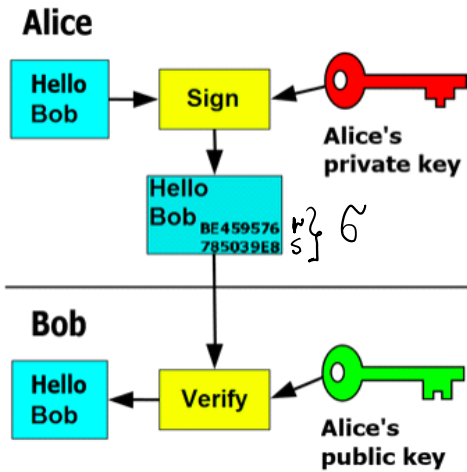
M - any message of finite length to be signed.

1. M is hashed with h-function H() hv

Signature Creation - Verification

$S = \text{Sign}(\text{Pr}K_A, h) = \sigma = (r, s)$

$V = \text{Ver}(\text{Pu}K_A, \sigma, h), V \in \{\text{True}, \text{False}\} \equiv \{1, 0\}$



IBM Hyperledger Fabric  
IBM Trust Food

Signature creation by sender 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:  $\sigma = \text{Sig}(\text{Pr}K_A, h) = (r, s)$ .

Signature verification:

1. Received message M' is hashed by receiver Bob  $h' = H(M')$ .
2. Signature is verified by verification function  $\text{Ver}(\text{Pu}K_A, \sigma, h')$ .

If  $\text{Pr}K_A = x, \text{Pu}K_A = a$  and  $a = g^x \text{ mod } p$

AND

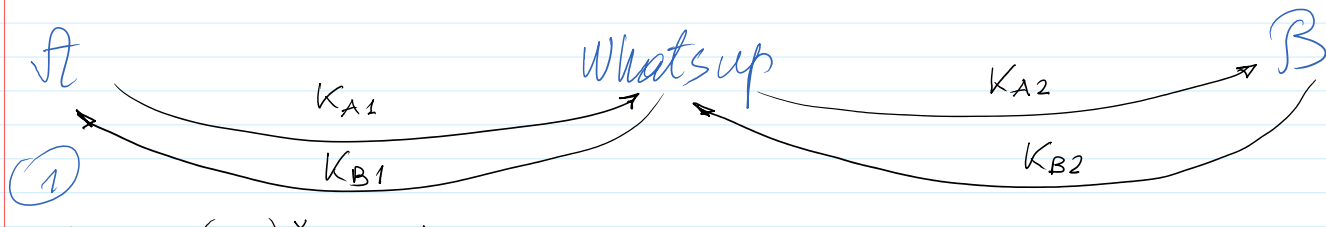
If  $M = M'$

Then signature is valid and  $V \in \{\text{True}\}$ .

Hash and Sign paradigm

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

M - message to be hashed  
 k - secret encr. key  
 $A(k)$        $B(k)$   
 A: wish to encr. message m together with providing its authenticity and integrity.



$$\textcircled{1} \quad \overbrace{K_{B1}} \quad \overbrace{K_{B2}}$$

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

$K_1$

$K_2$

M - message

$$\text{Enc}(K_1, m) = C_1 \longrightarrow$$

$$\text{Dec}(K_1, C_1) = m$$

Data center

$$\text{Enc}(K_2, m) = C_2 \longrightarrow$$

$$\text{Dec}(K_2, C_2) = m$$

$\textcircled{2}$  whatsapp software and its updating  
 ↓  
 Backdoors →

Chosen Plaintext Attack

A:

$$\left. \begin{array}{l} E_{CBC}(k, m) = c \\ H_{CBC}(k, c) = h \end{array} \right\} \begin{array}{l} \text{encrypt } c, h \\ \& \text{hash} \end{array} \longrightarrow$$

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

?  $h \neq h'$  if ok

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