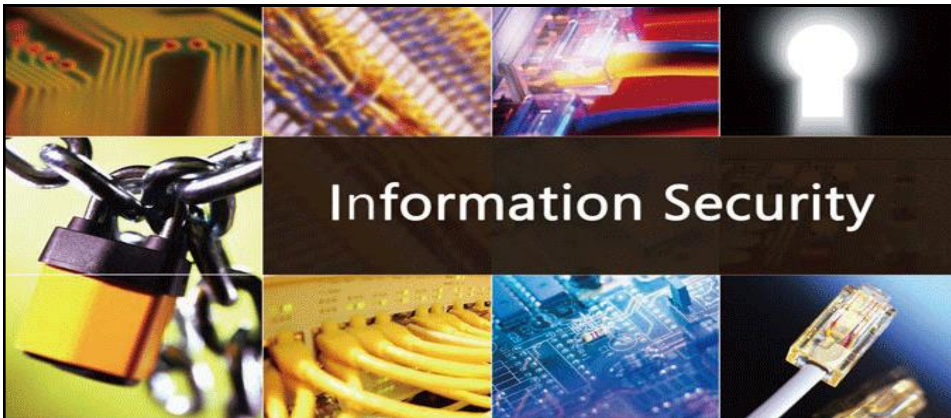


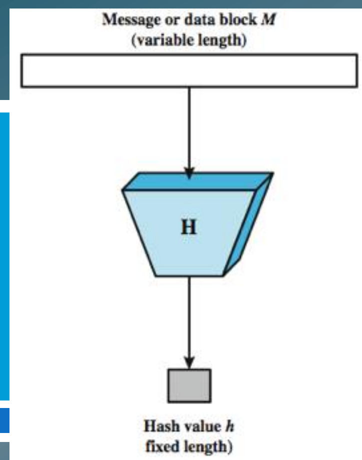
Integrity, Authentication message
Hash – MAC – HMAC – Digital Signature

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Contents

- Cryptographic Hash Functions
- Message Integrity checking
- Message Authentication - MAC
- Hashed Message Authentication Code - HMAC
- Digital Signature

Cryptographic Hash Functions



Nguyen Thi Thanh Van - Khoa CNTT

Cryptographic Hash Functions

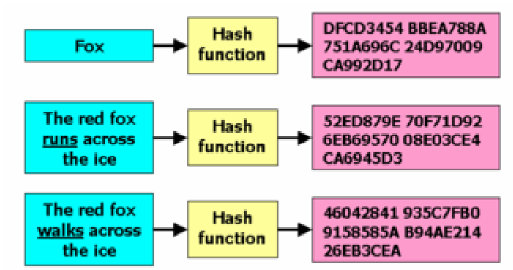
- What is Hash Functions
- Cryptographic Hash Function Criteria
- Iterated Hash Function
- Designing a hash function
- Secure Hash Algorithm (SHA): SHA-512
- Message Digest 5 - MD5
- Attacks on Hash Functions
- Application of Hash

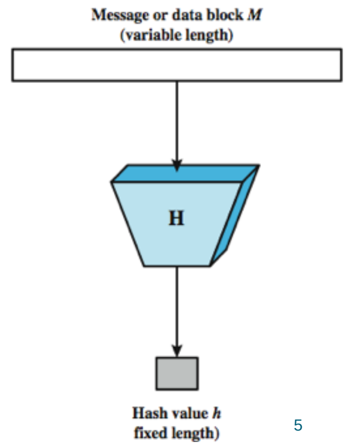
What is Hash Functions

- A hash function maps a *variable-length message* into a *fixed-length hash value*, or message digest

  ***h* = H(*M*)**

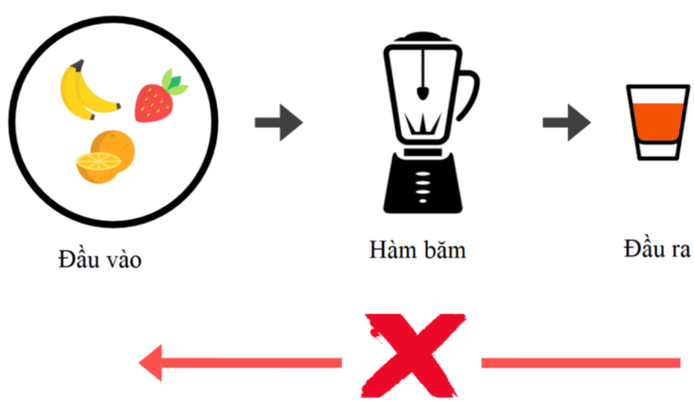
- The *principal object:*
  - *data integrity*



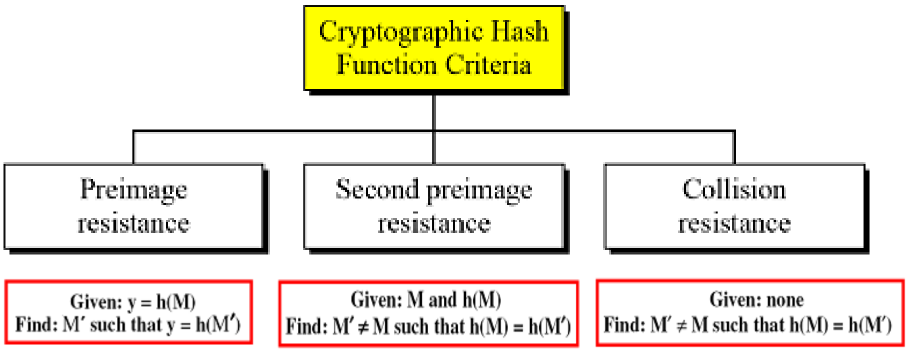


Hash

- One-way function

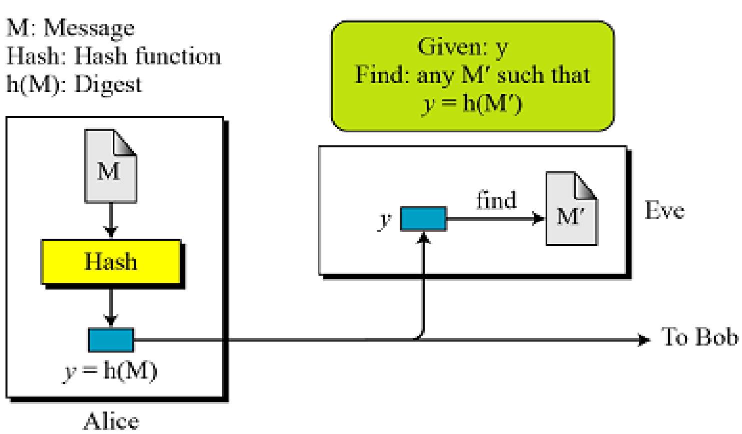


Cryptographic Hash Function Criteria



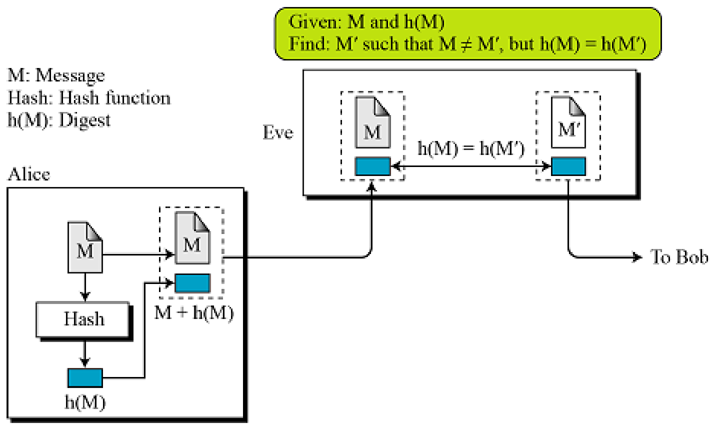
Preimage Resistance

- it must be extremely difficult for attacker to find any message, M′, such that y = h(M′).



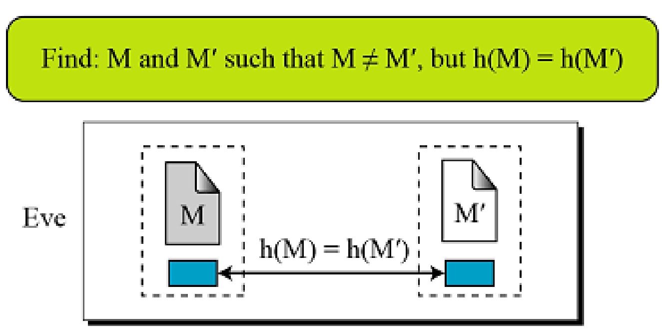
Second Preimage Resistance

- Attacker cannot easily create another message that hashes to the exact same digest



Collision Resistance

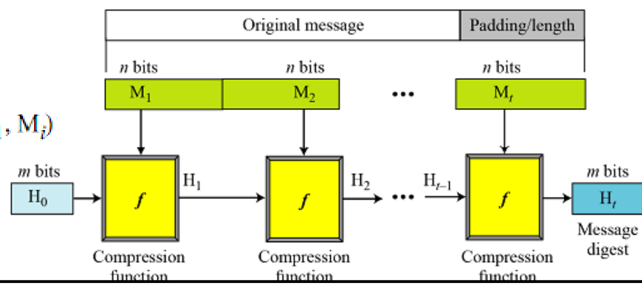
- ensures that attacker cannot find two messages that hash to the same digest.



Iterated Hash Function

- Iterated Hash Function
  - a function with fixed-size input is created.
  - It is referred to as a compression function: n-bit string to create an m-bit string where n is normally greater than m.
- Merkle-Damgard Scheme:
  - an iterated hash function that is collision resistant if the compression function is collision resistant.

$$H_i = f(H_{i-1}, M_i)$$



Designing a hash function

- In the first approach, the compression function is made from scratch:
  - Message Digest (MD): Several hash algorithms were designed by Ron Rivest.
    - MD2, MD4, and MD5,
  - Secure Hash Algorithm (SHA): The Secure Hash Algorithm (SHA) was developed by the NIST and FIP 180.
    - The standard is mostly based on MD5.
    - The standard was revised in 1995 under FIP180-1, which includes SHA-1.
    - It was revised later under FIP 180-2, which defines four new versions: SHA-224, SHA-256, SHA-384, and SHA-512. Table 12.1 lists some of the characteristics of these versions
- In the second approach, a symmetric-key block cipher serves as a compression function.
  - Whirlpool

SHA

- Characteristics of Secure Hash Algorithms (SHAs)

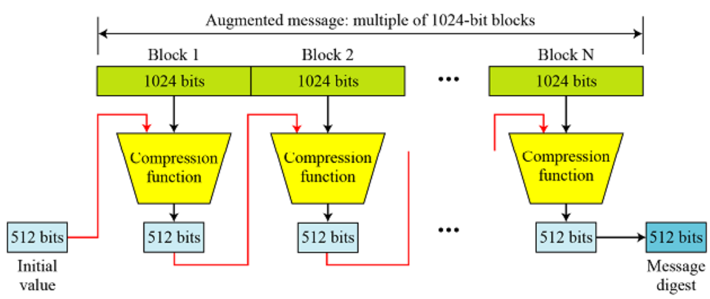
Characteristics	*SHA-1*	*SHA-224*	*SHA-256*	*SHA-384*	*SHA-512*
Maximum Message size	$2^{64}-1$	$2^{64}-1$	$2^{64}-1$	$2^{128}-1$	$2^{128}-1$
Block size	512	512	512	1024	1024
Message digest size	160	224	256	384	512
Number of rounds	80	64	64	80	80
Word size	32	32	32	64	64

Typical Hash

Thuật toán	*(output size)*	*Internal state size*	*Block size*	*Length size*	*(Word size)*	*(Collision)*
HAVAL	256/224/192/160/128	256	1024	64	32	Có
MD2	128	384	128	Không	8	khả năng lớı
MD4	128	128	512	64	32	Có
MD5	128	144	122	88	88	Có
PANAMA	256	8736	256	No	32	Có lỗi
RIPEMD	128	128	512	64	32	Có
RIPEMD-128/256	128/256	128/256	512	64	32	Không
RIPEMD-160/320	160/320	160/320	512	64	32	Không
SHA-0	160	160	512	64	32	Không
SHA-1	160	160	512	64	32	Có lỗi
SHA-256/224	256/224	256	512	64	32	Không
SHA-512/384	512/384	512	1024	128	64	Không
Tiger(2)-192/160/128	192/160/128	192	512	64	64	Không
VEST-4/8 (hash mode)	160/256	256/384	8	80/128	1	Không[1]
VEST-16/32 (hash mode)	320/512	512/768	8	160/256	1	Không
WHIRLPOOL	512	512	512	256	8	Không

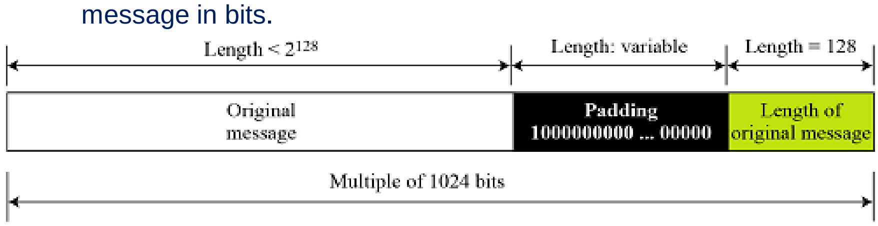
SHA-512

- SHA-512: is based on the Merkle-Damgard scheme.
- Operation:
  - initialize a predetermined value of 512 bits.
  - mixes IV with Block1 => MD1. Then mixes MD1 with Block2 =>MD2
  - Mixes the MDn-1with the Blockn => MDn.
  - Resulting digest is the message digest for the entire message.



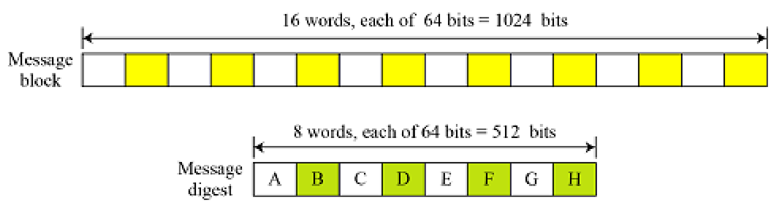
Operation of SHA-512

- Message Preparation:
  - SHA-512 insists that the length of the original message be less than 2128 bits.
- Length Field and Padding:
  - SHA-512 requires the addition of a 128-bit unsigned-integer length field to the message that defines the length of the message in bits.



Operation of SHA-512

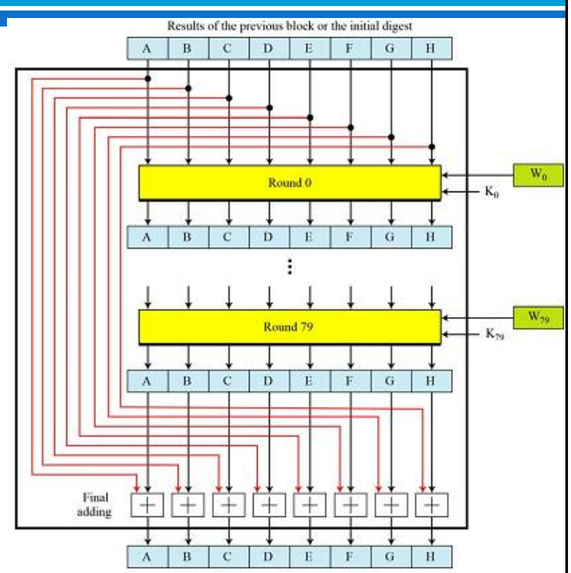
- Word oriented. SHA-512 operates on words
  - A word is defined as 64 bits.
  - each block of the message consists of 16 64-bit words.
  - The MD is also made of 64-bit words, but the MD is only 8 words and the words are named A, B, C, D, E, F, G, and H,



Operation of SHA-512

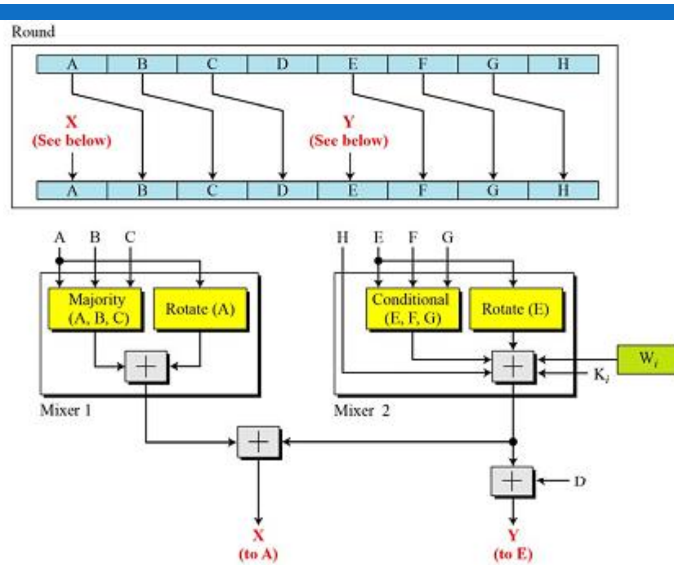
Compression Function

- 1 block: 80 rounds
- 1 round:
  - 8 buffers: are saved into 8 temporary variables.
  - 1word
  - 64-bit constant (Ki)
- Round 79:
  - All values are added to the values created from step 79



Operation of SHA-512

- Structure of each round



Message Digest 5 - MD5

- MD5, is a strengthened version of MD4 that divides the message into blocks of 512 bits and creates a 128-bit digest.
  - It turned out that a message digest of size 128 bits is too small to resist collision attack.
- Process:
  - Input: variable length
  - Output: Message digest 128 bits
  - 5 step on block 512 bits

  Step 1: Append Padding Bits

  Step 2. Append Length

  Step 3. Initialize MD Buffer

  Step 4. Process Message in 16-Word Blocks

  Step 5. Output

Attacks on Hash function

- two categories of attacks on hash functions:
  - Brute-force attack:
    - depend only on bit length of the hash value (not specific algorithm)
    - Attack to: One-way function; collision resistant - weak

    wishes to find a value y such that H(y)=h, try 2m-1 values
    - Attack to: collision resistant - strong

    wishes to find 2 messages: x,y, that yield H(y)=H(x), try 2m/2 values
  - Cryptanalysis:
    - based on weaknesses in a particular cryptographic algorithm.
    - require a cryptanalytic effort greater than or equal to the BF effort

Application of Hash

- Message Integrity checking
- Message Authentication
- HMAC - Hashed Message Authentication Code
- Digital Signature

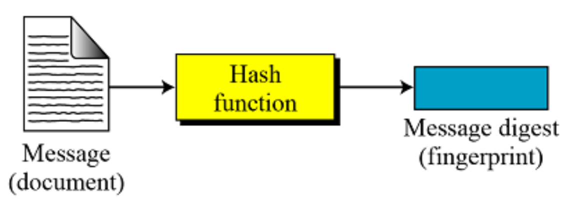
Message Integrity

ᘓ ᘐ

Nguyen Thi Thanh Van - Khoa CNTT

Message and Message Digest

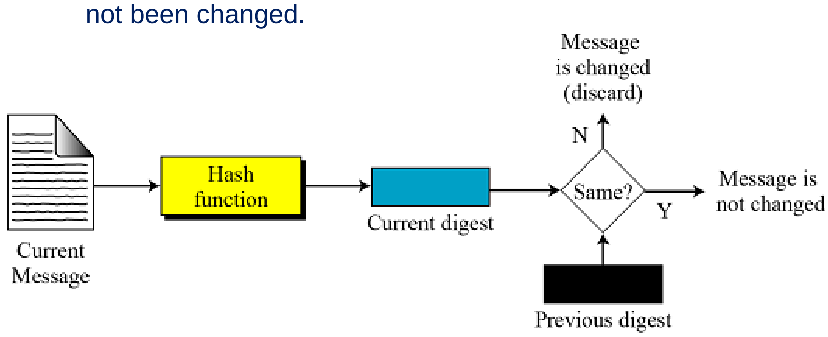
- The electronic equivalent of the document and fingerprint pair is the message and digest pair.
  - The document and fingerprint are physically linked together.
  - The message and message digest can be unlinked separately,



  - The message digest needs to be safe from change.

Checking integrity

- To check the integrity of a message, or document,
  - run the cryptographic hash function again and compare the new message digest with the previous one.
  - If both are the same, we are sure that the original message has not been changed.



Message authentication

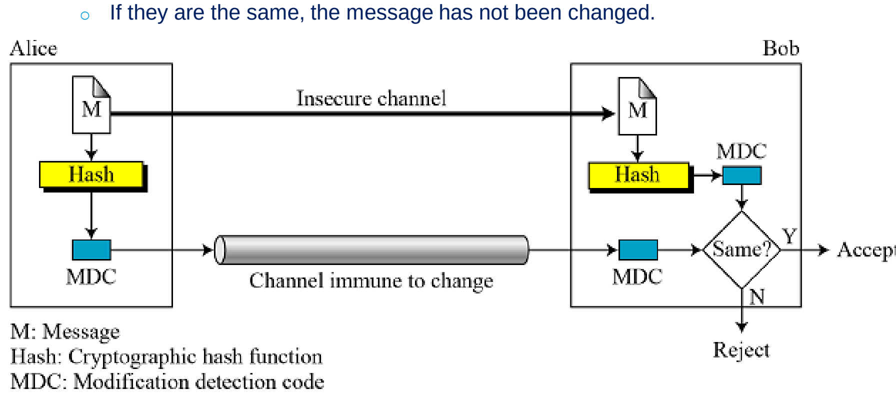
Nguyen Thi Thanh Van - Khoa CNTT

Message authentication

- A message digest does not authenticate the sender of the message.
- Message authentication: sender needs to provide proof that it is sender sending the message and not an impostor.
- The digest created by a cryptographic hash function is normally called a modification detection code (MDC).
- What we need for message authentication is a message authentication code (MAC).

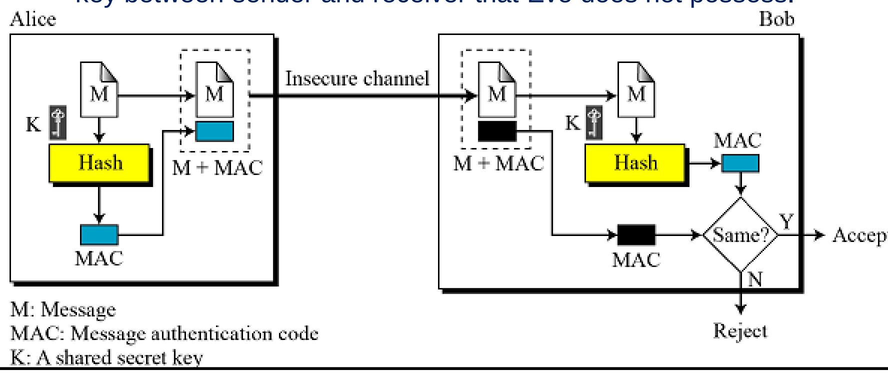
Modification detection code (MDC)

- (MDC) is a MD that can prove the integrity of the message
  - If Alice needs to send a message to Bob and create a MD, MDC, and send both the message and the MDC to Bob.
  - Bob can create a new MDC from the message and compare the received MDC and the new MDC.
  - If they are the same, the message has not been changed.



Message Authentication Code (MAC)

- To ensure the integrity of the message and the data origin authentication
  - change a MDC to a MAC.
  - The difference between a MDC and a MAC: MAC includes a secret key between sender and receiver that Eve does not possess.



Security of a MAC

- Attacker can forge a message without knowing the secret key?
  - 1. Eve may prepend all possible keys at the beginning of the message and make a digest of the (K|M) to find the digest equal to the one intercepted. She then knows the key and can replace the message with a forged message.
  - 2. The size of the key is normally very large in a MAC, but Eve can use another tool: the preimage attack – she finds X such that h(X) = MAC she has intercepted. => find the key and replace the message with a forged one.
  - 3. Given some pairs of messages and their MACs, Eve can manipulate them to come up with a new message and its MAC.
- The security of a MAC depends on the security of the underlying hash algorithm.

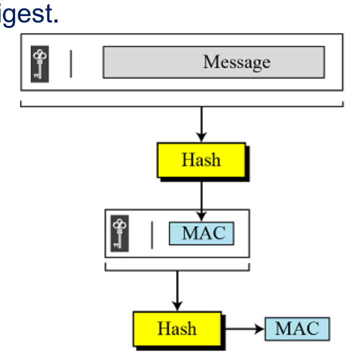
23/09/2021 30

Security of MAC

- two categories of attacks on MAC:
  - Brute-force attack:
    - depends on the relative size of the key and the tag
    - more difficult undertaking than BF attack on a hash function because it requires known message-tag pairs.
  - Cryptanalysis:
    - based on weaknesses in a particular cryptographic algorithm.
    - require a cryptanalytic effort greater than or equal to the BF effort
    - There is much more variety in the structure of MACs than in hash functions, so it is difficult to generalize about the cryptanalysis of MACs.

Nested MAC

- To improve the security of a MAC, nested MACs were designed in which hashing is done in two steps.
  - Step1: the key is concatenated with the message and is hashed to create an intermediate digest.
  - Step2: the key is concatenated with the intermediate digest to create the final digest.

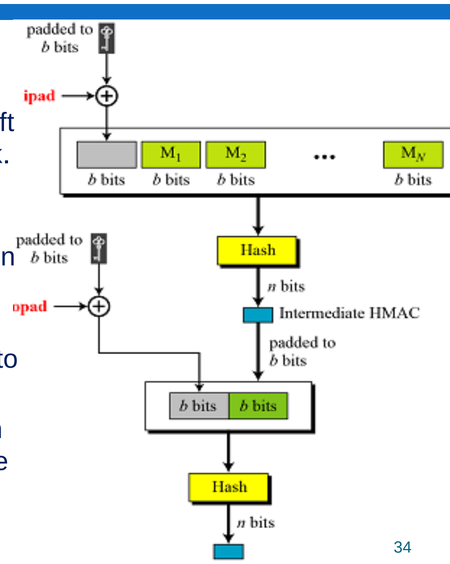


HMAC - Hashed MAC

- HMAC: a standard (FIPS 198) is issued by NIST
- The implementation of HMAC:
  - is much more complex than the simplified nested MAC
  - There are additional features, such as padding.
- The steps: see figure
  - 1. The message is divided into N blocks, each of b bits.
  - 2. The secret key is left-padded with 0's to create a b-bit key.
  - 3. The result of step 2 is XOR with a constant called ipad (input pad) to create a b-bit block. The value of ipad is the b/8 repetition of the sequence 00110110 (36 in hexadecimal).
  - 4. The resulting block is prepended to the N-block message. The result is N + 1 blocks.
  - 5. The result of step 4 is hashed to create an n-bit digest. We call the digest the inter mediate HMAC.

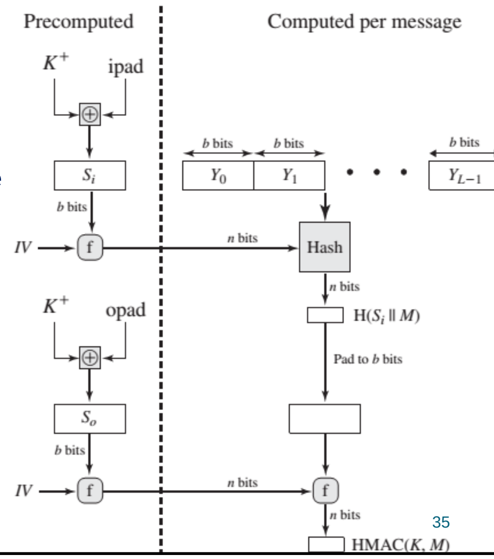
HMAC

- 6. The intermediate n-bit HMAC is left padded with 0s to make a b-bit block.
- 7. Steps 2 and 3 are repeated by a different constant opad (output pad). The value of opad is the b/8 repetition of the sequence 01011100 (5C in hexadecimal).
- 8. The result of step 7 is prepended to the block of step 6.
- 9. The result of step 8 is hashed with the same hashing algorithm to create the final n-bit HMAC.



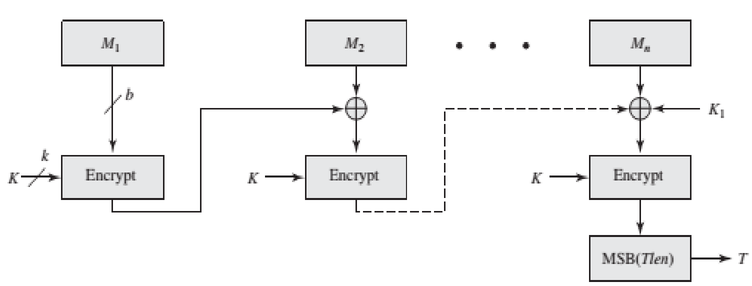
Security of HMAC

- based on an embedded hash function
  - depends on strength of the core hash function.
  - the probability of successful fake with time spent and some message–tag pairs created with the same key.
- Attack:
  - compute an output of the compression function
  - finds collisions in the hash function



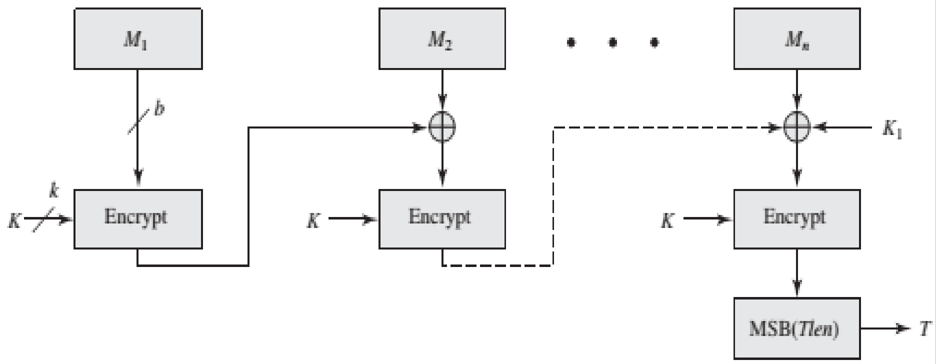
Cipher-Based Message Authentication Code (CMAC)

- operation for use with AES and triple DES:
- using three keys:
  - one key of length to be used at each step of the cipher block chaining and
  - two keys of length , where is the key length and is the cipher block length.
- This proposed construction: the two -bit keys could be derived from the encryption key, rather than being provided separately



(a) Message length is integer multiple of block size

Cipher-Based Message Authentication Code (CMAC)



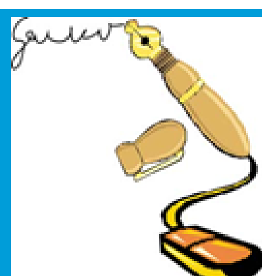
(a) Message length is integer multiple of block size

$$C_n = E(K, [M_n \oplus C_{n-1} \oplus K_1])$$
$$T = MSB_{Tlen}(C_n)$$

T = message authetication code, also referred to as the tag
$Tlen$ = bit length of T
$MSB_s(X)$ = the s leftmost bits of the bit string X

23/09/2021

Digital Signature



Nguyen Thi Thanh Van - Khoa CNTT

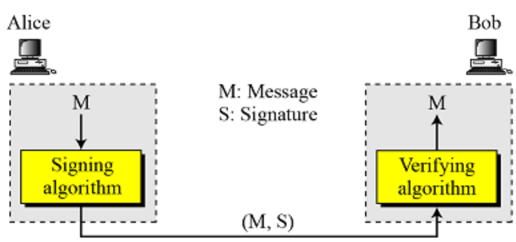
22/09/2021

Digital signature

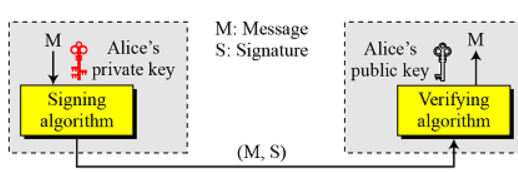
- A digital signature:
  - enables the creator of a message to attach a code that acts as a signature.
  - is formed by taking the hash of the message and encrypting the message with the creator's private key.

- digital signature properties:
  - verify the author and time of the signature.
  - authenticate the contents at the time of the signature.
  - It must be verifiable by third parties, to resolve disputes.

Digital signature process

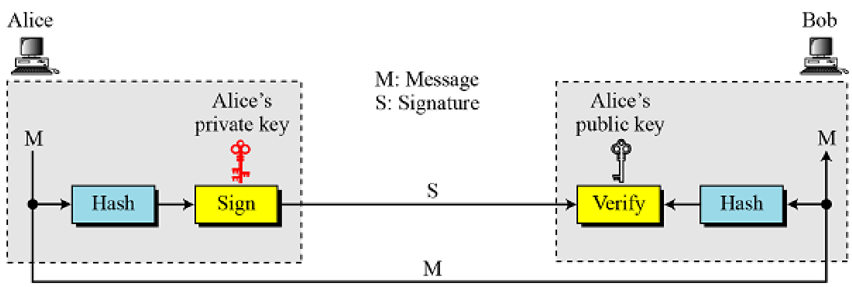


- Adding key to the digital signature process
  - needs a public-key system. The signer signs with her private key; the verifier verifies with the signer's public key.



Signing the digest

- The asymmetric-key cryptosystems: short messages.
- In a digital signature system, the messages are long
- => sign a digest of the message, which is much shorter than the message.
  - The sender can sign the MD and the receiver can verify the MD.
  - The effect is the same.

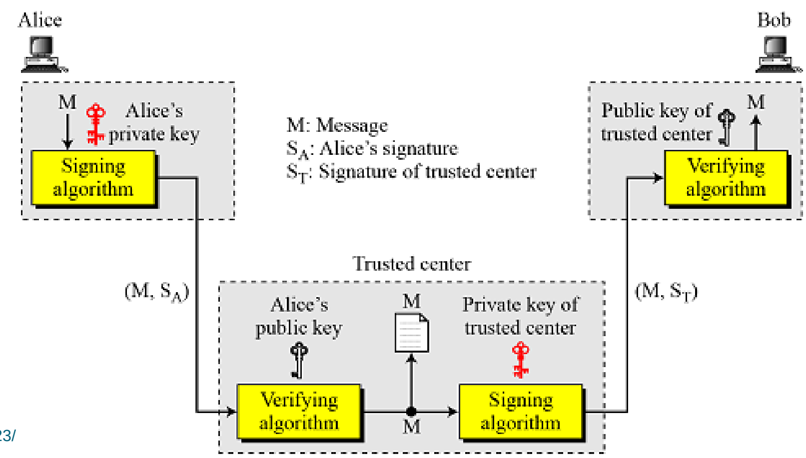


Security services

- A digital signature can directly provide several security services for message
  - Message Authentication
  - Message Integrity
  - Nonrepudiation
  - Confidentiality

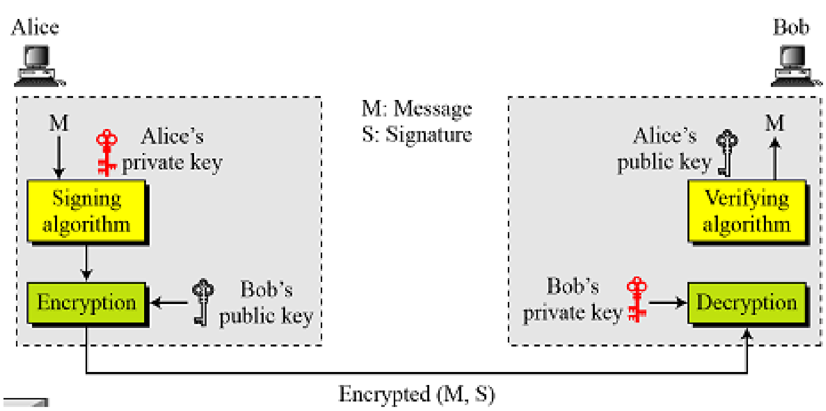
Security services

- Nonrepudiation can be provided using a trusted party.



Security services

- Confidentiality: is added to a digital signature scheme



Attacks on digital signature

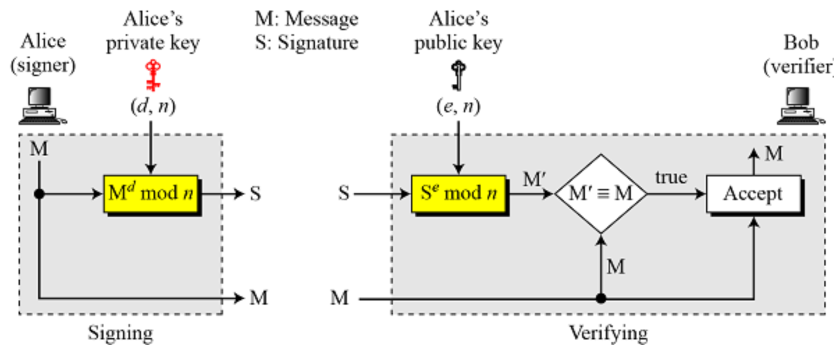
- Key-Only Attack
  - Eve has access only to the public information released by Alice. To forge a message, Eve needs to create Alice's signature to convince Bob that the message is coming from Alice. => the same as the ciphertext-only attack.
- Known-Message Attack
  - Eve has access to some documents previously signed by Alice. Eve tries to create another message and forge Alice's signature on it. => similar to the known-plaintext attack.
- Chosen-Message Attack
  - Eve somehow makes Alice sign one or more messages for her. Eve now has a chosen-message/signature pair. Eve later creates another message, with the content she wants, and forges Alice's signature on it. => similar to the chosen-plaintext attack.

Digital signature schemes

- RSA Digital Signature Scheme
- ElGamal Digital Signature Scheme
- Schnorr Digital Signature Scheme
- Digital Signature Standard (DSS)
- Elliptic Curve Digital Signature Scheme

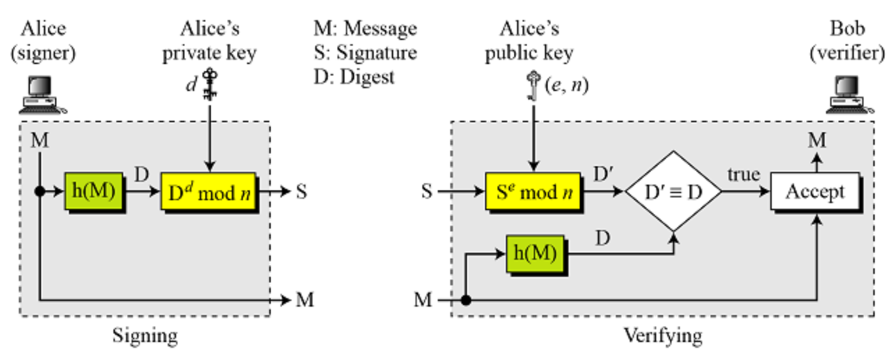
RSA Digital Signature Scheme

- RSA can also be used for signing and verifying a message
  - The signing and verifying sites use the same function, but with different parameters.
  - Signing: use private key (d,n)
  - Verifying: use pblic key (e,n)



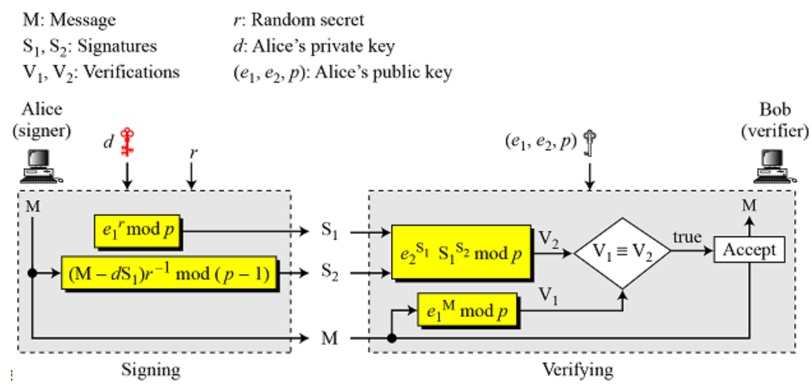
The RSA signature on the MD

- When the digest is signed instead of the message itself, the susceptibility of the RSA digital signature scheme depends on the strength of the hash algorithm.



ElGamal digital signature scheme

- Signing: 2 functions create two signatures
- Verifying the outputs of 2 functions are compared

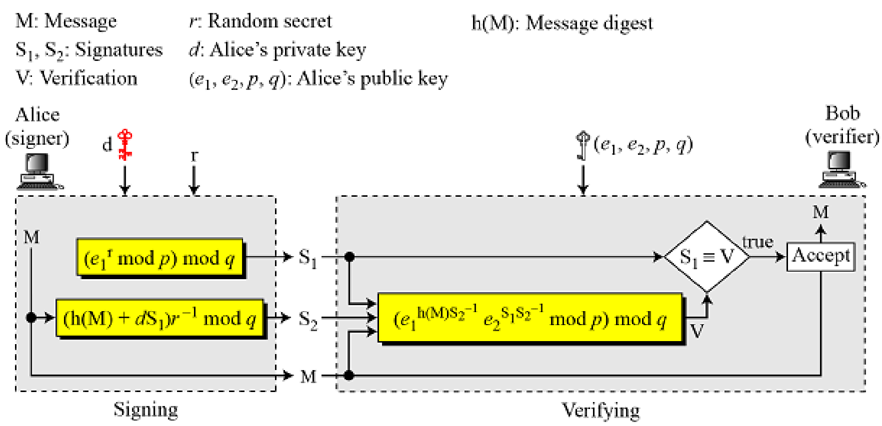


Digital Signature Standard DSS

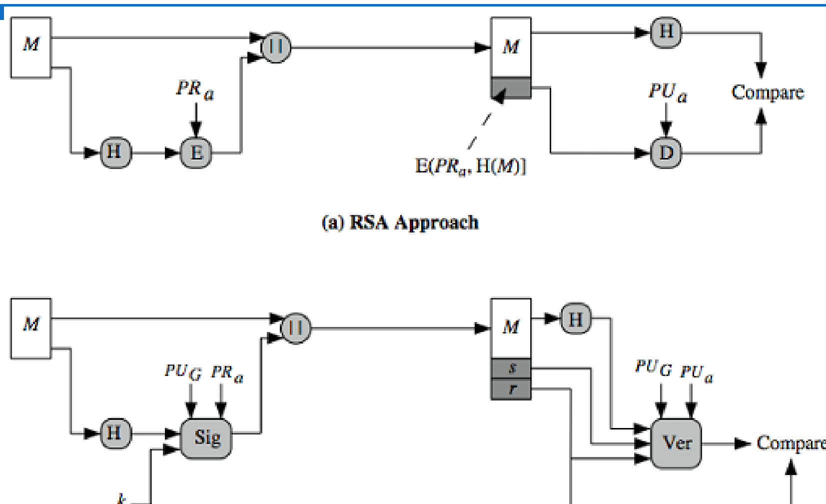
- DSS: Digital Signature Standard
  - US Govt approved signature scheme
  - designed by NIST & NSA in early 90's
  - published as FIPS-186 in 1991, revised in 1993, 1996, 2000
  - Use RSA to create the digital signature process
- DSA: Digital Signature Algorithm
  - new digital signature technique
  - is a public-key technique

DSS scheme

- DSS Versus RSA: Computation of DSS signatures is faster than computation of RSA signatures when using the same p.



RSA vs. DSS



(a) RSA Approach

(b) DSS Approach

DSS uses an algorithm that is designed to provide only the digital signature function

it cannot be used for encryption

Practice openSSL

- **Secure Sockets Layer (SSL)** is an application-level protocol which was developed by the Netscape Corporation for the purpose of transmitting sensitive information, such as Credit Card details, via the Internet
- **OpenSSL** is a robust, commercial-grade implementation of SSL tools, and related general-purpose library based upon SSL, developed by Eric A. Young and Tim J. Hudson
- OpenSSL is already installed on SEEDUbuntu

Q & A