Asymmetric Cryptography
Cryptographic Primitives

Design and Verification of Security Protocols and Security Ceremonies

Programa de Pós-Graduacão em Ciências da Computacão
Dr. Jean Everson Martina

August-November 2016

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

Message Authentication Codes

- They couple the idea of an integrity checking functions with shared key crypto-system;

Message Authentication Codes

- They couple the idea of an integrity checking functions with shared key crypto-system;
- They are also length reducing functions;

Message Authentication Codes

- They couple the idea of an integrity checking functions with shared key crypto-system;
- They are also length reducing functions;
- They are publicly known;

Message Authentication Codes

- They couple the idea of an integrity checking functions with shared key crypto-system;
- They are also length reducing functions;
- They are publicly known;
- And ease of computation.

MAC Functions' Properties

- Given n pairs $(m_1, MAC_k(m_1))$,..., $(m_n, MAC_k(m_n))$ find a new pair $(m, MAC_k(m))$ efficiently and with non negligible probability is unlikely;

MAC Functions' Properties

- Given n pairs $(m_1, MAC_k(m_1))$,..., $(m_n, MAC_k(m_n))$ find a new pair $(m, MAC_k(m))$ efficiently and with non negligible probability is unlikely;
- Output should be a length-reduction function;

MAC Functions' Properties

- Given n pairs $(m_1, MAC_k(m_1))$,..., $(m_n, MAC_k(m_n))$ find a new pair $(m, MAC_k(m))$ efficiently and with non negligible probability is unlikely;
- Output should be a length-reduction function;
- The key should control the mapping between the Domain and Image of the MAC function, but not determine its spread.

MAC Construction

- There are basically two mains ways of producing secure MAC systems:

MAC Construction

- There are basically two mains ways of producing secure MAC systems:
  - Symmetric CBC-MAC;

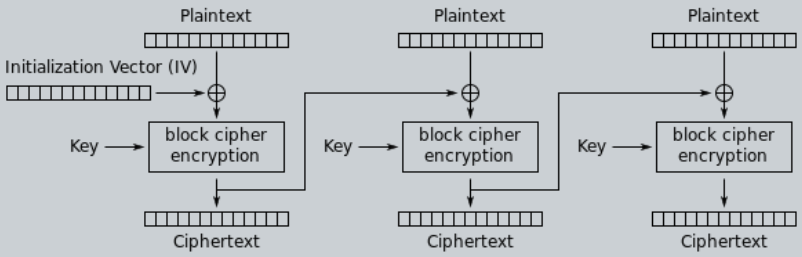
MAC Construction

- There are basically two mains ways of producing secure MAC systems:
  - Symmetric CBC-MAC;
  - CMAC;

MAC Construction

- There are basically two mains ways of producing secure MAC systems:
  - Symmetric CBC-MAC;
  - CMAC;
  - Hash based HMAC;

CBC-MAC Mode of Encryption

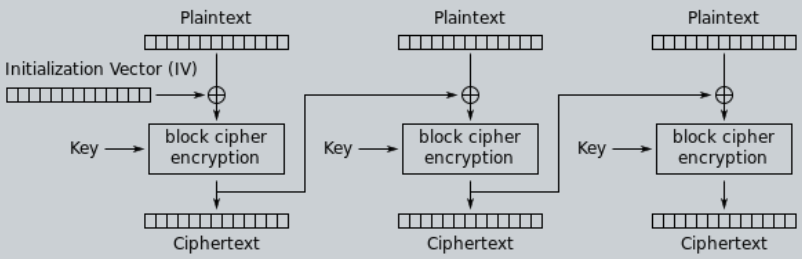


Cipher Block Chaining (CBC) mode encryption

;

- It is basically the application of CBC over input data;

CBC-MAC Mode of Encryption

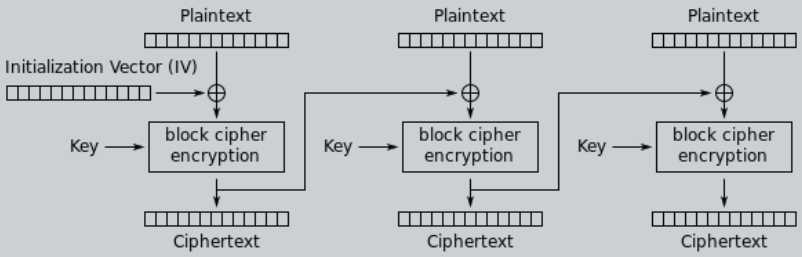


Cipher Block Chaining (CBC) mode encryption

;

- It is basically the application of CBC over input data;
- Instead of keeping all the blocks we just keep the last one;

CBC-MAC Mode of Encryption

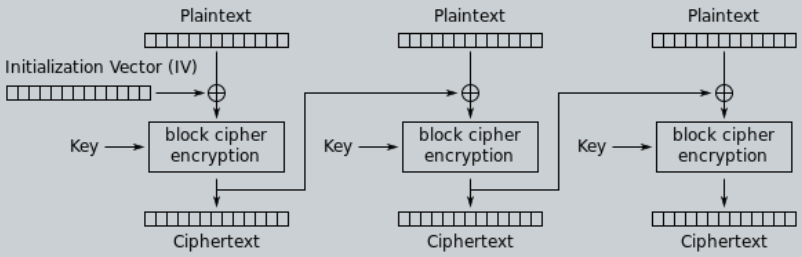


Cipher Block Chaining (CBC) mode encryption

;

- It is basically the application of CBC over input data;
- Instead of keeping all the blocks we just keep the last one;
- Its length is determined by block size;

CBC-MAC Mode of Encryption



Cipher Block Chaining (CBC) mode encryption

;

- It is basically the application of CBC over input data;
- Instead of keeping all the blocks we just keep the last one;
- Its length is determined by block size;
- IV is fixed.

Security of CBC-MAC

- Secure for messages of a fixed number of blocks assuming the block cipher is Pseudo-Random Permutation;

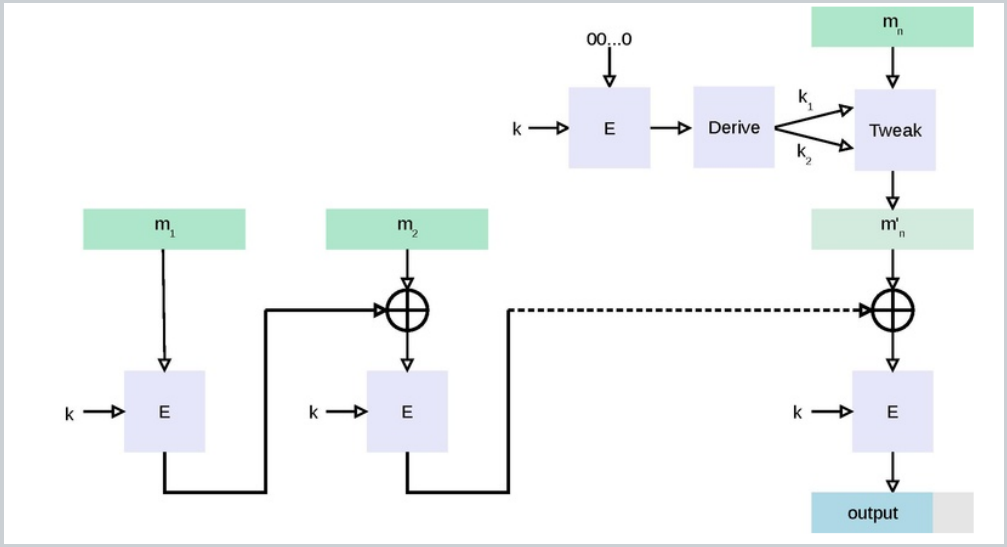
Security of CBC-MAC

- Secure for messages of a fixed number of blocks assuming the block cipher is Pseudo-Random Permutation;
- Not secure with variable lengths;

Security of CBC-MAC

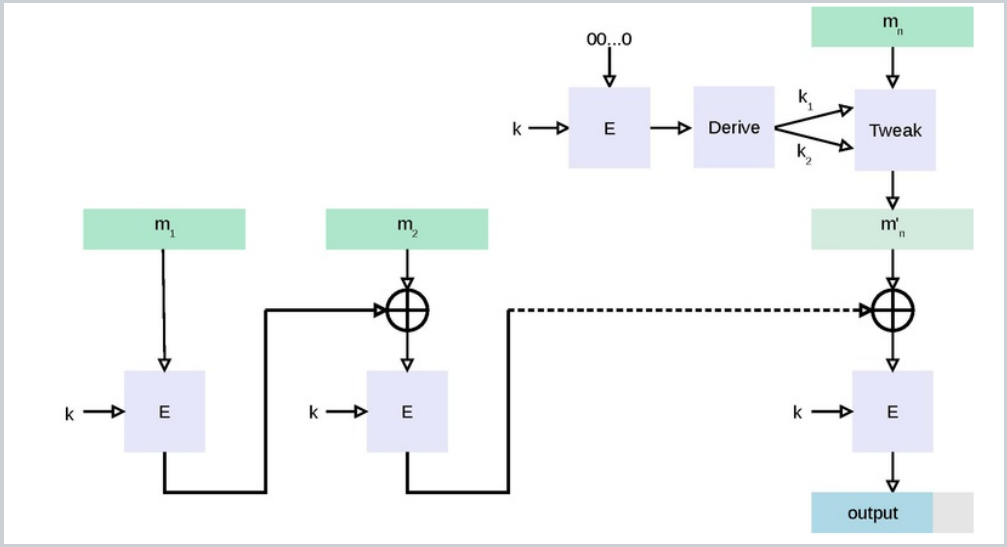
- Secure for messages of a fixed number of blocks assuming the block cipher is Pseudo-Random Permutation;
- Not secure with variable lengths;
- Needs to be used with one key to each message length or do length pre-pending;

CMAC



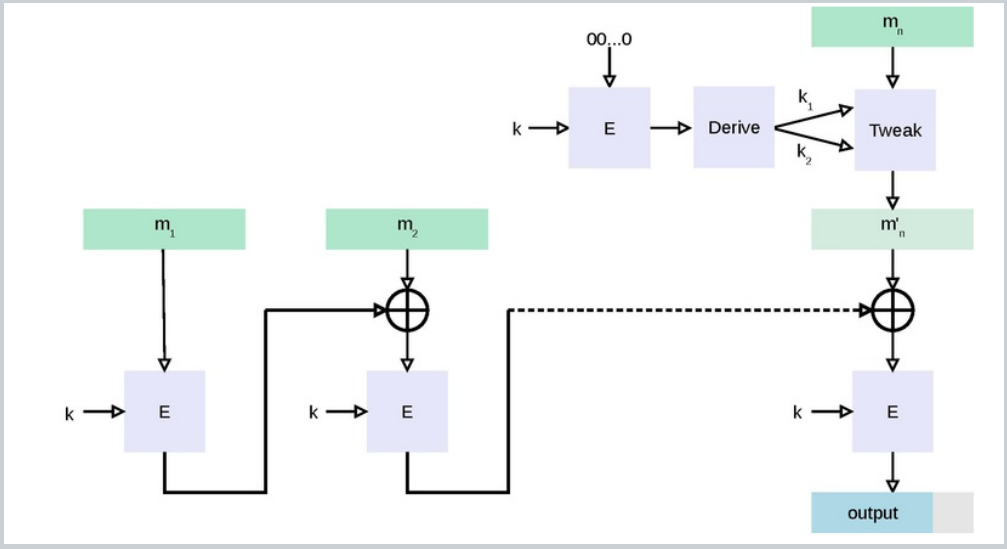
- It is a NIST standard for doing MAC with symmetric cyphers;

CMAC



- It is a NIST standard for doing MAC with symmetric cyphers;
- Efficiently addresses the security deficiencies of CBC-MAC;

CMAC



- It is a NIST standard for doing MAC with symmetric cyphers;
- Efficiently addresses the security deficiencies of CBC-MAC;
- Derives 2 keys to cypher the last block;

HMAC Properties

- Use available hash functions without modification;

HMAC Properties

- Use available hash functions without modification;
- Preserve the original performance of the hash function;

HMAC Properties

- Use available hash functions without modification;
- Preserve the original performance of the hash function;
- Use and handle keys in a simple way;

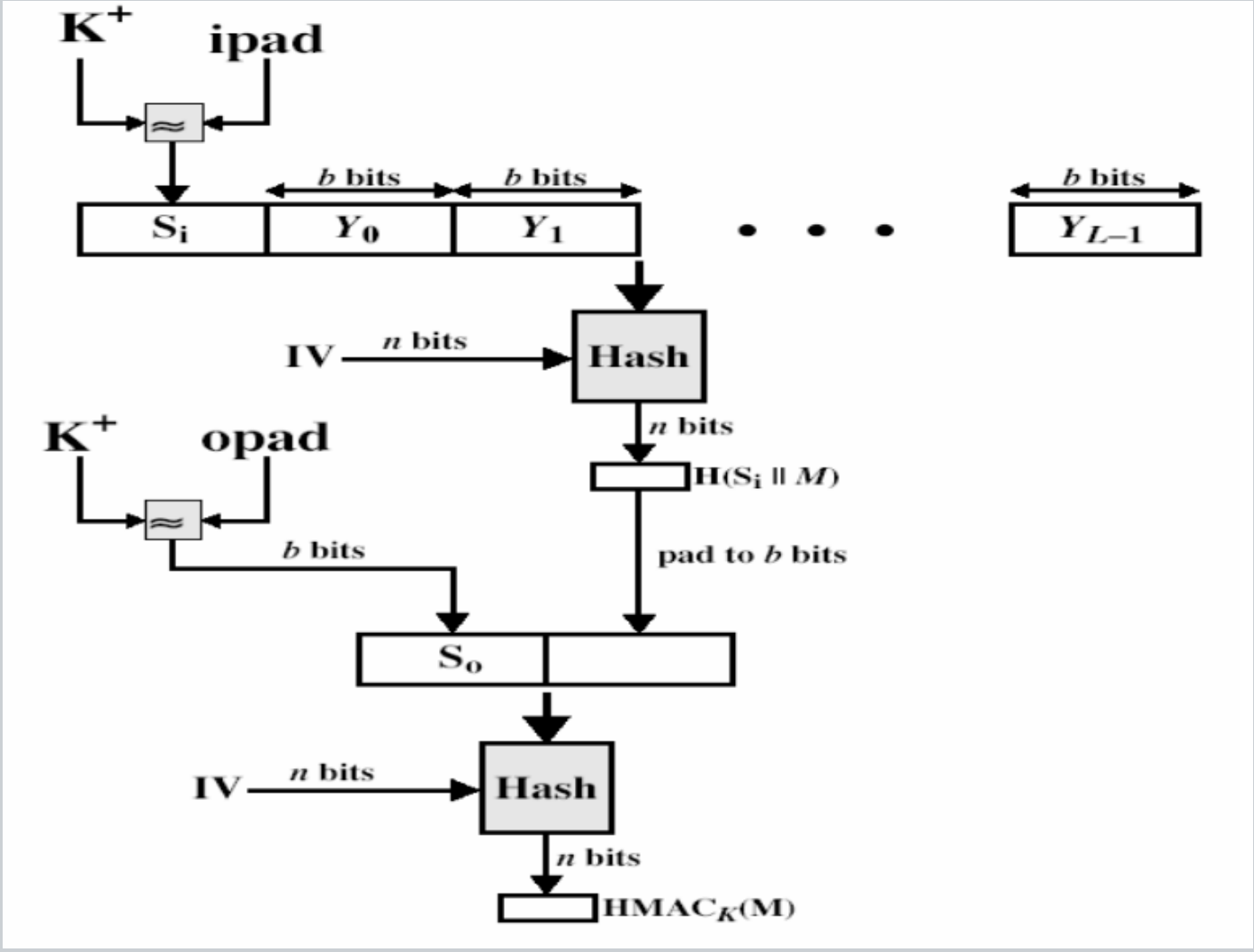
HMAC Properties

- Use available hash functions without modification;
- Preserve the original performance of the hash function;
- Use and handle keys in a simple way;
- Allow easy replacement of the underlying hash function;

HMAC Properties

- Use available hash functions without modification;
- Preserve the original performance of the hash function;
- Use and handle keys in a simple way;
- Allow easy replacement of the underlying hash function;
- Have a well-understood analysis of the strength of the authentication mechanisms;

HMAC


K+
ipad
b bits
b bits
b bits
Si
Y0
Y1
YL–1
IV
n bits
Hash
n bits
K+
opad
H(Si || M)
b bits
pad to b bits
So
IV
n bits
Hash
n bits
HMACK(M)

Security of HMAC

- Security of HMAC relates to that of the underlying hash algorithm;
- If used with a secure hash functions and according to the specification (key size, and use correct output), no known practical attacks;

Asymmetric Cryptography

- Appeared on the 1970s. First classified by GCHQ and later publicly by Diffie and Helmann's work;

Asymmetric Cryptography

- Appeared on the 1970s. First classified by GCHQ and later publicly by Diffie and Helmann's work;
- Comes to solve the secure distribution channel on symmetric cryptography;

Asymmetric Cryptography

- Appeared on the 1970s. First classified by GCHQ and later publicly by Diffie and Helmann's work;
- Comes to solve the secure distribution channel on symmetric cryptography;
- A user has two keys: a public key and a private key;

Asymmetric Cryptography

- Appeared on the 1970s. First classified by GCHQ and later publicly by Diffie and Helmann's work;
- Comes to solve the secure distribution channel on symmetric cryptography;
- A user has two keys: a public key and a private key;
- Usually it is thousand of times more computationally intensive than symmetric cryptography.

Asymmetric Crypto-system Properties

- A message can be encrypted with the public key and decrypted with the private key to provide security;

Asymmetric Crypto-system Properties

- A message can be encrypted with the public key and decrypted with the private key to provide security;
- A message can be encrypted with the private key and decrypted with the public key to provide signatures;

Asymmetric Crypto-system Properties

- A message can be encrypted with the public key and decrypted with the private key to provide security;
- A message can be encrypted with the private key and decrypted with the public key to provide signatures;
- Security is related to strong mathematical problems;

Asymmetric Crypto-system Properties

- A message can be encrypted with the public key and decrypted with the private key to provide security;
- A message can be encrypted with the private key and decrypted with the public key to provide signatures;
- Security is related to strong mathematical problems;
- Usually these problems are both polynomial time, but there can be a trapdoor to solve it quickly;

Asymmetric Crypto-system Properties

- A message can be encrypted with the public key and decrypted with the private key to provide security;
- A message can be encrypted with the private key and decrypted with the public key to provide signatures;
- Security is related to strong mathematical problems;
- Usually these problems are both polynomial time, but there can be a trapdoor to solve it quickly;
- A lot of theoretical work compared to symmetric cryptography;

Asymmetric Crypto-system Properties

- A message can be encrypted with the public key and decrypted with the private key to provide security;
- A message can be encrypted with the private key and decrypted with the public key to provide signatures;
- Security is related to strong mathematical problems;
- Usually these problems are both polynomial time, but there can be a trapdoor to solve it quickly;
- A lot of theoretical work compared to symmetric cryptography;
- Usually based on finite fields constrained by modular operations.

Asymmetric Crypto-system Properties

- A message can be encrypted with the public key and decrypted with the private key to provide security;
- A message can be encrypted with the private key and decrypted with the public key to provide signatures;
- Security is related to strong mathematical problems;
- Usually these problems are both polynomial time, but there can be a trapdoor to solve it quickly;
- A lot of theoretical work compared to symmetric cryptography;
- Usually based on finite fields constrained by modular operations.

Private Keys

- There is a strong assumption on it possession;

Private Keys

- There is a strong assumption on it possession;
- Properties yielded are related to its owners executing his will;

Private Keys

- There is a strong assumption on it possession;
- Properties yielded are related to its owners executing his will;
- Strong mathematical relation between itself and it public counterpart;

Private Keys

- There is a strong assumption on it possession;
- Properties yielded are related to its owners executing his will;
- Strong mathematical relation between itself and it public counterpart;
- Finding it by random should be possible negligible probability;

Private Keys

- There is a strong assumption on it possession;
- Properties yielded are related to its owners executing his will;
- Strong mathematical relation between itself and it public counterpart;
- Finding it by random should be possible negligible probability;
- Derive it either from cypher-text and from public key should not be possible;

Private Keys

- There is a strong assumption on it possession;
- Properties yielded are related to its owners executing his will;
- Strong mathematical relation between itself and it public counterpart;
- Finding it by random should be possible negligible probability;
- Derive it either from cypher-text and from public key should not be possible;
- Provides authentication but does not provide confidentiality.

Public Keys

- There is a strong assumption on relation to identity;

Public Keys

- There is a strong assumption on relation to identity;
- Properties yielded are related to its other verifying the owners will;

Public Keys

- There is a strong assumption on relation to identity;
- Properties yielded are related to its other verifying the owners will;
- Strong mathematical relation between itself and it private counterpart;

Public Keys

- There is a strong assumption on relation to identity;
- Properties yielded are related to its other verifying the owners will;
- Strong mathematical relation between itself and it private counterpart;
- It should be as public as possible;

Public Keys

- There is a strong assumption on relation to identity;
- Properties yielded are related to its other verifying the owners will;
- Strong mathematical relation between itself and it private counterpart;
- It should be as public as possible;
- Does not provide authentication but only confidentiality.

Key Space

- Way bigger than symmetric cryptography;

Key Space

- Way bigger than symmetric cryptography;
- Usually this happens because not everything can be a key;

Key Space

- Way bigger than symmetric cryptography;
- Usually this happens because not everything can be a key;
- To operate with all mathematical properties the filed should be constructed over the idea of primality;

Key Space

- Way bigger than symmetric cryptography;
- Usually this happens because not everything can be a key;
- To operate with all mathematical properties the filed should be constructed over the idea of primality;
- Primality can be defined in different ways for different fields;

Key Space

- Way bigger than symmetric cryptography;
- Usually this happens because not everything can be a key;
- To operate with all mathematical properties the filed should be constructed over the idea of primality;
- Primality can be defined in different ways for different fields;
- Modular Exponentiation and Discrete Logarithm are the problems;

Key Space

- Way bigger than symmetric cryptography;
- Usually this happens because not everything can be a key;
- To operate with all mathematical properties the filed should be constructed over the idea of primality;
- Primality can be defined in different ways for different fields;
- Modular Exponentiation and Discrete Logarithm are the problems;
- Keys are defined for these operations.

Digital Signatures Mode

- Yields Authenticity of messages;

Digital Signatures Mode

- Yields Authenticity of messages;
- Desirable properties of a digital signature:

Digital Signatures Mode

- Yields Authenticity of messages;
- Desirable properties of a digital signature:
  - A receiver must be able to validate the signature;

Digital Signatures Mode

- Yields Authenticity of messages;
- Desirable properties of a digital signature:
  - A receiver must be able to validate the signature;
  - The signature must not be forgeable;

Digital Signatures Mode

- Yields Authenticity of messages;
- Desirable properties of a digital signature:
  - A receiver must be able to validate the signature;
  - The signature must not be forgeable;
  - The signer must not be able to repudiate the signature;

Digital Signatures Mode

- Yields Authenticity of messages;
- Desirable properties of a digital signature:
  - A receiver must be able to validate the signature;
  - The signature must not be forgeable;
  - The signer must not be able to repudiate the signature;
- Encrypt with private key, validate with public key;

Digital Signatures Mode

- Yields Authenticity of messages;
- Desirable properties of a digital signature:
  - A receiver must be able to validate the signature;
  - The signature must not be forgeable;
  - The signer must not be able to repudiate the signature;
- Encrypt with private key, validate with public key;
- For security and authenticity, encrypt the signed message with the receiver's public key;

Encryption Mode

- Yields Confidentiality of messages;

Encryption Mode

- Yields Confidentiality of messages;
- Guarantees the intended destination of a message;

Encryption Mode

- Yields Confidentiality of messages;
- Guarantees the intended destination of a message;
- Strongly related to the possession of the private key;

Encryption Mode

- Yields Confidentiality of messages;
- Guarantees the intended destination of a message;
- Strongly related to the possession of the private key;
- Usually has problems with messages bigger than key sizes;

Encryption Mode

- Yields Confidentiality of messages;
- Guarantees the intended destination of a message;
- Strongly related to the possession of the private key;
- Usually has problems with messages bigger than key sizes;

Questions????

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

UNIVERSIDADE FEDERAL
DE SANTA CATARINA