Criptografia e Segurança em Redes

网络加密和安全

Symmetric Encryption

Criptografia Simétrica

对称加密

What is Cryptography

O que é Criptografia?

什么是密码学?

The discipline that embodies the principles, means, and methods for the transformation of data to hide their semantic content, prevent their unauthorised use, or prevent undetected modification.

Criptografia é a disciplina que incorpora（混合，合并，一体） os princípios, meios e métodos para a transformação de dados com o objetivo de ocultar（隐藏，潜伏） seu conteúdo semântico（语义）, evitar seu uso não autorizado ou prevenir modificações（修改） não detectadas.

密码学是一门学科，包括将数据进行转换以隐藏其语义内容、防止未经授权的使用或防止未被察觉的修改的原则、手段和方法。

It aims at protecting security properties / 它的目标是保护安全性质 /Seu objetivo é proteger propriedades de segurança

• Confidentiality	• Confidencialidade	• 机密性
• Integrity	• Integridade	• 完整性
• Availability	• Disponibilidade	• 可用性
• Authenticity	• Autenticidade	• 真实性
• Non-repudiation	• Não-repúdio	• 不可否认性

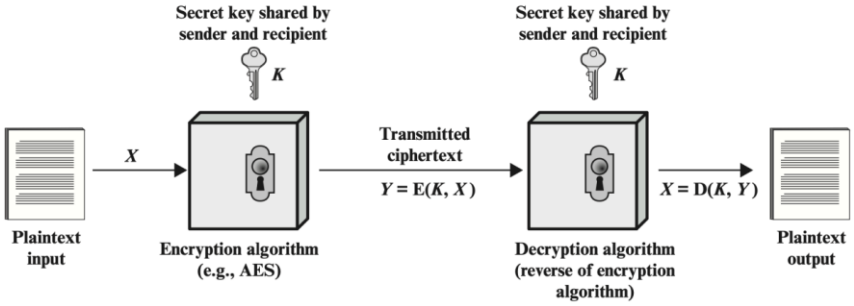
Principles 原则

- **Plaintext**: the original message or data fed into a cryptographic algorithm as input.
- **Encryption algorithm**: a set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key.
- **Secret key**: an input the encryption algorithm uses to perform the substitutions and transformation in the plaintext.
- **Ciphertext**: the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.
- **Decryption algorithm**: a set of rules that take the ciphertext and the secret key to produce the original plaintext. This is essentially the encryption algorithm run in reverse.

- **Texto Puro (Plaintext):** A mensagem original ou os dados inseridos em um algoritmo criptográfico como entrada.
- **Algoritmo de Criptografia**: Um conjunto de regras expressas matematicamente para tornar os dados ininteligíveis executando uma série de conversões controladas por uma chave.
- **Chave Secreta (Secret Key):** Uma entrada que o algoritmo de criptografia usa para realizar as substituições e transformações no texto puro.
- **Texto Cifrado (Ciphertext):** A mensagem embaralhada produzida como saída. Isso depende do texto puro e da chave secreta. Para uma mensagem dada, duas chaves diferentes produzirão dois textos cifrados diferentes.
- **Algoritmo de Descriptografia:** Um conjunto de regras que usam o texto cifrado e a chave secreta para produzir o texto puro original. Essencialmente, é o algoritmo de criptografia sendo executado em reverso.

- **明文 (Plaintext):** 原始消息或作为输入输入到加密算法中的数据。
- **加密算法:** 一组以数学方式表达的规则，通过执行一系列受密钥控制的转换来使数据变得不可理解。
- **密钥 (Secret Key):** 加密算法用来执行明文中的替代和转换的输入。
- **密文 (Ciphertext):** 作为输出产生的混淆消息。它取决于明文和密钥。对于给定的消息，两个不同的密钥将产生两个不同的密文。
- **解密算法:** 一组规则，使用密文和密钥来生成原始明文。本质上，它是加密算法的逆向运行。

Simplified Model of Symmetric Encryption



Attacks on Cryptographic Systems

Ataques a Sistemas Criptográficos

加密系统的攻击

"The objective is either to recover the plaintext or the secret key in use."

"O objetivo é recuperar o texto puro ou a chave secreta em uso."

"其目标要么是恢复明文，要么是获取正在使用的密钥。"

Cryptanalysis Rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs. The known characteristics are used to deduce a specific plaintext or the secret key.

Brute-force attack The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

Criptoanálise

A criptoanálise depende da natureza do algoritmo, e talvez de algum conhecimento das características gerais do texto puro ou até mesmo de algumas amostras de pares de texto puro-texto cifrado. As características conhecidas são usadas para deduzir um texto puro específico ou a chave secreta.

Ataque de Força Bruta

No ataque de força bruta, o atacante tenta todas as chaves possíveis em um pedaço de texto cifrado até obter uma tradução inteligível em texto puro. Em média, metade de todas as chaves possíveis deve ser testada para obter sucesso.

密码分析

密码分析依赖于算法的特性，也许还有一些关于明文的一般特性或甚至一些明文-密文对的知识。已知的特性用于推断特定的明文或秘密密钥。

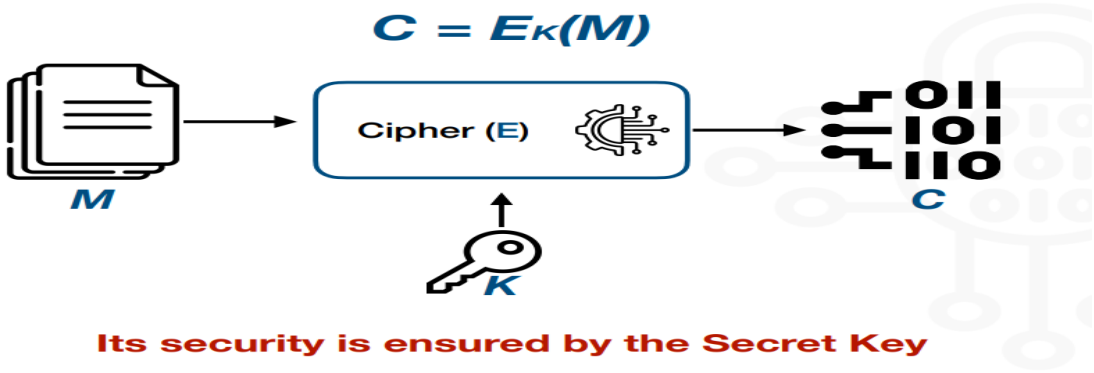
穷举攻击 在穷举攻击中，攻击者尝试在一段密文上尝试所有可能的密钥，直到获得明文的可理解翻译。平均来说，必须尝试一半的所有可能密钥才能取得成功。

Kerckhoff's Principle 克克霍夫原则

"A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."

"Um criptossistema deve ser seguro mesmo que tudo sobre o sistema, exceto a chave, seja do conhecimento público."

"一个加密系统应该是安全的，即使系统的所有信息，除了密钥之外，都是公开的。"



An encryption scheme is **unconditionally secure** if the ciphertext generated by the scheme does not contain enough information to recover the corresponding plaintext, no matter how much ciphertext is available and how much time an attacker has.

An encryption scheme is **computationally secure** if the ciphertext generated by the scheme meets one or both of the following criteria:

- The cost of breaking the cipher exceeds the value of the encrypted information;
- The time required to break the cipher exceeds the useful lifetime of the information.

Um esquema de criptografia é **incondicionalmente seguro** se o texto cifrado gerado pelo esquema não contém informações suficientes para recuperar o texto puro correspondente, não importando o quanto de texto cifrado esteja disponível e quanto tempo um atacante tenha.

Um esquema de criptografia é **computacionalmente seguro** se o texto cifrado gerado pelo esquema atende a um ou ambos dos seguintes critérios:

- O custo de quebrar o cifrado excede o valor das informações criptografadas;
- O tempo necessário para quebrar o cifrado excede o tempo de vida útil das informações.

一个加密方案如果生成的密文不含足够信息来恢复相应的明文，无论攻击者拥有多少密文和时间，就被称为**无条件安全**。

一个加密方案如果生成的密文满足以下一个或两个条件，就被称为**计算上安全**：

- 破解密码的成本超过了加密信息的价值；
- 破解密码所需的时间超过了信息的有用寿命

Classical Techniques / Técnicas Clássicas /经典技术

Caesar Cipher / Cifra de César / 凯撒密码

Funciona substituindo cada letra do alfabeto pela letra que está três posições adiante no alfabeto.

它通过用字母表中比原字母向下三个位置的字母来替换每个字母来运作。

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Example

Plaintext: attackatnineam

Ciphertext: DWWDFNDWQLQHDP

26 possible keys.
One of them is insecure.

It is possible to use an arbitrary offset (key).

Plaintext: attackatnineam

Ciphertext (k=6): GZZGIQGZTOTKGS

Algorithm

By assigning a numerical equivalent to each letter, the algorithm can be expressed as follows:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

For each plaintext p, substitute the ciphertext letter C:

$$C = E(k,p) = (p + k) \bmod 26$$

The decryption algorithm is:

$$p = D(k,C) = (C - k) \bmod 26$$