Escuela Colombiana de Ingeniería Julio Garavito

Demo Company
IT Security and Privacy

Crytography

Student:
Laura Sofia Gil Chaves

Teacher:
Ing. Daniel Vela

Business Confidential

October 02th, 2024
Project 01-11
Version 1.0

Table of Contests

Assessment Overview

From Thursday, September 26 to Monday, September 30, an analysis of various cryptographic techniques was carried out using the Windows system, with the objective of better understanding methods such as Breaking the Shift Cipher, Breaking the Mono-alphabetic Substitution Cipher, One-Time Pad and Perfect Secrecy, Message Authentication Codes and Cryptographic Hash Functions and Applications. This analysis included the study of these cryptographic algorithms and the evaluation of their applications and vulnerabilities.

1.Planning: Identification of the steps required to analyze cryptographic techniques and understand their vulnerabilities.

2.Discovery: Exploration of tools used to implement the techniques and understand how they work.

3.Attacking: Practical application of methods to break ciphers and analyze their security.

4.Reporting: Recording of the analysis of cryptographic techniques.

Plan → Discovery → Attack →Report

Assessment Components

- *Breaking the Shift Cipher:*

  Is a simple method that consists of shifting each letter of the message a fixed number of positions in the alphabet. Its simplicity makes it vulnerable to brute-force attacks or frequency analysis, since it is easy to identify common patterns in the language of the encrypted message. This component will evaluate how to break this cipher by applying these techniques.

- *Breaking the Mono-alphabetic Substitution Cipher:*

  This cipher replaces each letter of the original text with another letter of the alphabet in a consistent manner. Although it is more complex than the shift cipher, it is still vulnerable to frequency analysis, since the most common letters in the message language will appear with the same frequency in the ciphertext. The evaluation will focus on demonstrating how to use this analysis to decrypt the message and expose its weaknesses.

- *One-Time Pad and Perfect Secrecy:*

The one-time pad is a cipher that, when used correctly, offers perfect secrecy, meaning that it is theoretically impossible to break. However, if the key is reused or is not truly random, the cipher becomes vulnerable. This component will evaluate both the performance of the one-time pad under ideal conditions and the common errors that compromise its security.

- *Message Authentication Codes (MAC):*

  MACs are used to guarantee the integrity and authenticity of messages. How they function in providing a signature to verify that the content has not been altered during transmission is evaluated. Potential vulnerabilities to spoofing attacks and the conditions under which a MAC could be compromised will also be analyzed.

- *Cryptographic Hash Functions and Applications:*

  Cryptographic hash functions convert data of any size into a fixed-length hash value. They are essential in data integrity verification and in the creation of digital signatures. This component will evaluate the properties of hash functions, such as collision resistance, and their use in security applications, highlighting how these functions can be vulnerable to certain attacks if not used properly.

Scope

Assessment	Details
External Penetration Test	cse29-iiith.vlabs.ac.in

Scope Exclusions

No scope exclusions will be established for cryptographic techniques, as all testing will be conducted in a secure and controlled laboratory environment. The primary focus will be on the practical application of cryptographic techniques.

Client Allowances

The permissions necessary to perform cryptographic testing will be provided by the cse29-iiith.vlabs.ac.in page, which will allow full access to all files and resources necessary for analysis and experimentation with cryptographic techniques.

Security Weaknesses

- *Breaking the Shift Cipher:*

  The shift cipher is extremely weak because it only shifts letters in the alphabet by a fixed amount. This makes it vulnerable to brute force attacks, as there are a limited number of possible shifts (26 in the English alphabet). An attacker can try all combinations quickly. More complex encryption algorithms, such as symmetric encryption, can be implemented, which offer a higher level of security through longer keys and a more sophisticated encryption approach.

- *Breaking the Mono-alphabetic Substitution Cipher:*

  This method is still vulnerable to frequency analysis. In many languages, certain letters appear more frequently with this an attacker can identify which letters correspond to which letters in the ciphertext, significantly weakening the security of the cipher. A cipher can be implemented that uses multiple alphabets and substitution patterns, making frequency analysis more difficult and improving message security.

- *One-Time Pad and Perfect Secrecy:*

  The weakness of the one-time pad lies in its practical implementation, since it requires the key to be truly random, if the message and used only once. To ensure its effectiveness, it is to establish a secure method for the generation and distribution of keys, guaranteeing that they are not reused and that they are completely random.

- *Message Authentication Codes (MAC):*

  The security of MACs depends on the strength of the keys and the underlying algorithm. If the key is compromised or the algorithm is weak, attackers can spoof messages. A robust and secure algorithm must be used to generate MACs, and adequate protection of the keys used must be ensured by implementing key rotation and secure key storage policies.

- *Cryptographic Hash Functions and Applications:*

  Hash functions can be vulnerable to collision attacks, especially if older versions such as MD5 or SHA-1 are used. The solution is to adopt secure, up-to-date hash functions, such as SHA-256 or SHA-3, which offer collision resistance and are widely accepted in security applications, thus ensuring data integrity and protection against attacks.

External Penetration Test Findings

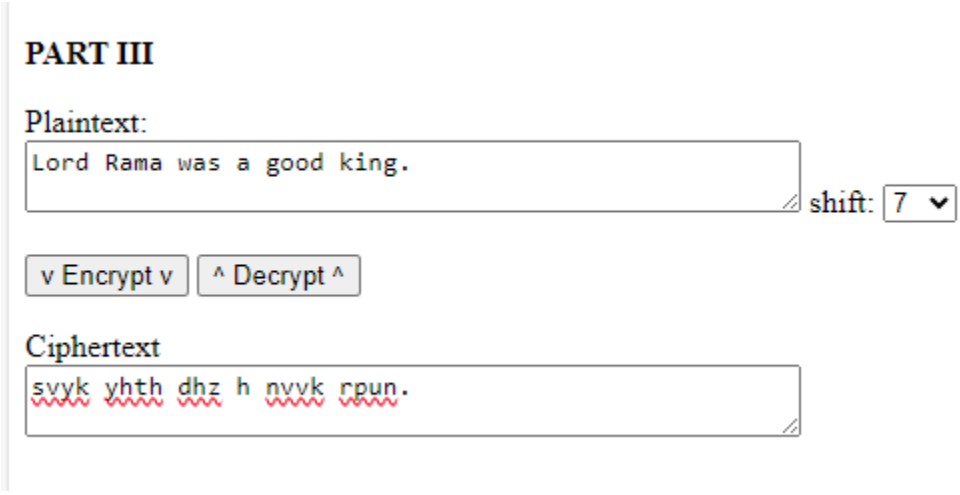
External Penetration Test Findings

Description:	Cryptographic techniques studied included shift encryption, which is vulnerable to brute force attacks, and mono-alphabetic substitution encryption, which is susceptible to frequency analysis. The one-time pad is effective, but requires rigorous implementation of truly random, single-use keys. Message Authentication Codes (MAC) rely on key protection, while hash functions are vulnerable to collision attacks.
Impact:	Critical
System:	Windows
References:	cse29-iiith.vlabs.ac.in

Exploit Proof of Concept

Breaking the shift cipher

1. Encrypt the following plain text using key k = 7.
   Plain Text : Lord Rama was a good king.
   Answer: svyk yhth dhz h nvvk rpun



2. Given a plain text and its corresponding cipher text, find out the key used for the encryption of the plain text.
   Plain Text : abcdefghijklmnopqrstuvwxyz
   Cipher Text : TDNUCBZROHLGYVFPWIXSEKAMQJ

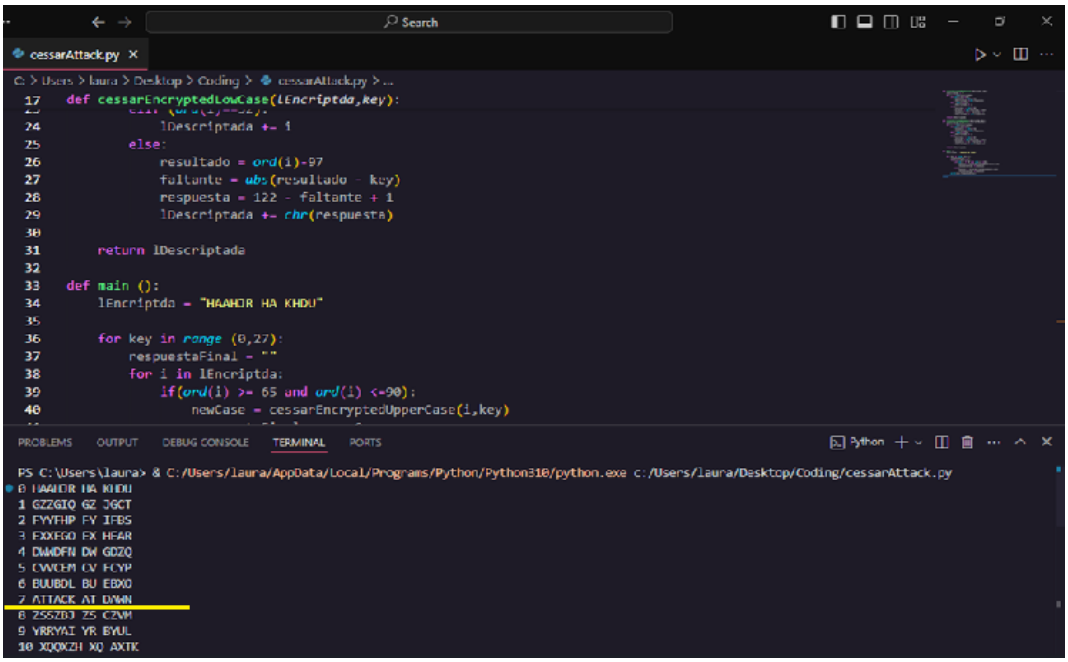
Answer: Cannot be performed because the keys are not the same in any case.

```
>>> abs(ord("a") - ord("T"))
13
>>> abs(ord("b") - ord("D"))
30
>>> abs(ord("c") - ord("N"))
21
>>> abs(ord("d") - ord("U"))
15
>>>
```

3. How many different keys are possible with an n-letter alphabet?

Each value of a can has 26 different addition shifts (the b value); therefore, there are 12 × 26 or 312 possible keys.

4. Given a cipher text, find out the corresponding plain text using brute force attack.
   Cipher text : HAAHJR HA KHDU
   Answer: ATTACK AT DAWN



Breaking the Mono Alphabetic Substitution Cipher

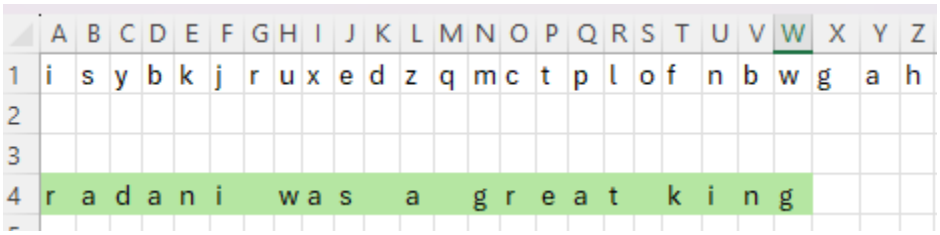
1. Encrypt the following plain text using the key given
   Plain Text: Lord Rama was a great king.
   Key: abcdef ghi jk l mnopqr st uv wxyz
   Answer: yUSR rJGJ LJS J CSKW QOAC

2. What is the key space if we use alphabet = {a,b,c,d,e,f}

   In a monoalphabetic cipher, each letter of the alphabet can be replaced by any other letter of the alphabet without repetition, which implies that the total number of possible keys is equivalent to the number of possible permutations of the letters of the alphabet.

   If we use the alphabet {a, b, c, d, e, f}, this alphabet has 6 letters. To calculate the key space, we need to find the number of possible permutations of these 6 letters, which is calculated as the factorial of 6: $6!=6\times5\times4\times3\times3\times2\times1=720$, then the key space is 720 possible different keys.

3. Decrypt the following cipher text with the key given
   Cipher Text : libimi wio i rlkif dxmr
   Key: abcdefghijklmnopqrstuvwxyz
   isybkjruxedzq mct plofnbwgah
   Answer: radani was a great king



	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
1	i	s	y	b	k	j	r	u	x	e	d	z	q	m	c	t	p	l	o	f	n	b	w	g	a	h
2																										
3																										
4	r	a	d	a	n	i		w	a	s		a		g	r	e	a	t		k	i	n	g			

Vernam Cypher and Perfect secrecy

1. Prove that if only a single character is encrypted, then the shift cipher is perfectly secret.

   The Vernam cipher (one-time pad) is considered perfectly secret when only a single character is encrypted, as it uses a random key of the same length as the plaintext. The encryption operation is performed by adding modulo N, where each character in the ciphertext can be generated from N possible combinations of plaintext characters and keys. This means that for a given ciphertext character C, all plaintext characters are

equally likely, implying that the probability of a character Pi given C is the same as its original probability, P(Pi|C)=P(Pi). Therefore, the Vernam cipher provides perfect secrecy, as no information about the plaintext can be deduced from the ciphertext.

2. What is the largest plaintext space M you can find for which the mono-alphabetic substitution cipher provides perfect secrecy? (Note: M need not contain only valid English words.)

   Mono-alphabetic substitution encryption cannot provide perfect secrecy for a large message space, since the number of possible keys is limited to 26 permutations in the case of the English alphabet, which is not sufficient to cover all possible message combinations. For perfect secrecy to be achieved, the message space M would have to be extremely small, so that the number of possible messages is equal to or less than the number of available keys. In that case, each message could have a unique key, thus fulfilling the perfect secrecy requirement, but in large message spaces, this is not possible.

3. Show how to use the Vigenère cipher to encrypt any word of length t so that perfect secrecy is obtained (Note: you can choose the length of the key).

   To obtain perfect secrecy with the Vigenère cipher, a random key of the same length as the message must be used. In this case, each letter of the message is encrypted by adding it to the corresponding letter of the key using mod 26, in the case of the English alphabet. Since the key is completely random and is used only once, each ciphertext can correspond to any possible message, making it impossible to decrypt the original message without knowing the key, thus fulfilling the criterion of perfect secrecy.

Message Authentication Code (CBC-MAC)

1. If a MAC tag is K-bits long, how much work is needed to find a collision to that specific value.
   (a) 2^{k/2}
   (b)K^2
   (c) K!
   (d) K^K

   This refers to the birthday attack, where the amount of work required to find a collision is proportional to 2^{k/2}, where K is the length in bits of the MAC tag.

2. The output length of SHA – I is _____ bits
   (a) 128
   (b) 16
   (c) 64
   (d) 256

   None of the answers, SHA-1 produces a 160-bit hash value, so its output length is always 160 bits.

3. Best way to achieve both privacy and message integrity
   (a) Encrypt and Authenticate
   (b) Authenticate then Encrypt
   (c) Encrypt then Authenticate
   (d) All

   The recommended approach to combine privacy and integrity is to encrypt first and then authenticate. This methodology is considered more secure since authenticating the message after encryption protects against certain types of cryptographic attacks.

Cryptographic Hash Functions and Applications (HMAC)

1. Which criterion ensures that we can't find two messages that hash to the same digest?
   (a) One-wayness
   (b) Weak-collision-resistance
   (c) Strong-collision-resistance
   (d) None

   It ensures that it is extremely difficult to find two different messages that produce the same hash value.

2. Which criterion Ensures that it must be extremely difficult or impossible to create the message if the message digest is given.
   (a) One-wayness
   (b) Weak-collision-resistance
   (c) Strong-collision resistance
   (d) None

   This criterion means that, given a digest, it is computationally infeasible to find the original message.

3. The Merkle-Damgard Transform is mainly useful for
   (a) Converting any fixed-length collision resistant hash function to an arbitrary length collision resistant hash function
   (b) Converting arbitrary length hash function to a fixed length hash function
   (c) Constructing hash function from random function
   (d) None

   This approach allows a fixed-length hash function to process variable-length inputs while maintaining collision resistance.

4. Understand HMAC scheme and find a break it is using available source code.

   It is a mechanism that combines a cryptographic hash function with a secret key to provide message authentication and integrity. HMAC is based on the use of a hash function, such as SHA-256, and is structured in such a way that any change to the message or secret key would alter the resulting digest. To “break” HMAC, an attacker would need to obtain the secret key, which is extremely difficult if a key of sufficient length and randomness is used.

5. Understand Merkel-Damgard transform and Explain, how we are using it for HMAC?

   The Merkle-Damgard transformation allows a variable-length hash function to be constructed from a fixed-length hash function. HMAC uses this transformation to ensure that the message and the key are processed in a way that maintains security. In the HMAC scheme, the message is concatenated with the key and processed through the hash function in two steps: first, a hash of the key concatenated with the message is calculated, and then, the hash is again applied to the key and the resulting hash of the message

6. Explain why HMAC is secure and on what assumptions this security is based?

   HMAC is considered secure due to its resistance to collision and pre-image attacks, as well as its dependence on the robustness of the underlying hash function. The security of HMAC is based on two assumptions: first, that the hash function used is collision resistant and, second, that the secret key is kept secure and is not predictable. If the hash function is adequate and the key is sufficiently long and random, HMAC provides a high level of security for message authentication.

References

- https://www.sciencedirect.com/topics/mathematics/message-authentication-code
- https://es.wikipedia.org/wiki/Secure_Hash_Algorithm
- https://en.wikipedia.org/wiki/Merkle–Damgård_construction
- https://es.wikipedia.org/wiki/HMAC