Information Security Technologies COMP607 Tutorial

Session 1 – Introduction and classical ciphers Introduction:

1. Which of these situations would require protection for CIA?

|  |  |  |  |
| --- | --- | --- | --- |
|  | C | I | A |
| Exam question file sent by email for printing | □ | □ | □ |
| Exam results posted on notice board | □ | □ | □ |
| Letter from your employer: | □ | □ | □ |
| about your payrise | □ | □ | □ |
| about your promotion | □ | □ | □ |
| about new staff joining | □ | □ | □ |
| A file in your computer storing your passwords | □ | □ | □ |
| Online newspaper report | □ | □ | □ |

1. Give some examples where Kerchoffs’s principle is (i) applied, (ii) not applied.

(i)Applied:

* **Cryptographic Protocols**: Kerckhoffs's Principle is applied in the design of cryptographic protocols to ensure security.
* **Encryption Key Security**: The principle emphasizes the importance of keeping the encryption key secure for overall system security.

(ii)Not applied:

* **Secrecy-Dependent Cryptosystems**: If any part of a cryptosystem, except the individual secret key, has to be kept secret, violating Kerckhoffs's Principle, the system is considered not secure.
* **Failure to Prioritize Key Security**: Systems that rely on the secrecy of the algorithm rather than the encryption key for security do not adhere to Kerckhoffs's Principle

1. What is them main requirement for the key according to Kerchoffs’s principle?

The essential need for the key in a cryptographic system, according to Kerckhoffs' Principle, is that the system's security should rely on the secrecy of the key, not the secrecy of the algorithm or any other component. The concept emphasizes that a cryptosystem should be secure even if everything about it, except the key, is known to the public. In essence, the key becomes a fundamental component in preserving the secrecy and security of encrypted data.

1. Encrypt the following message “ENEMY PLANE SPOTTED” using:

(a). Ceasar's cipher

(b). Vignere cipher using key: SUNSHINE

Use (i) graphical method, (ii) numerical method

(a). Ceasar's cipher:

(i) graphical method:

Key: 3

Plaintext: ENEMY PLANE SPOTTED

Ciphertext: HQHPB SODQH VSRWWHG

(ii) numerical method: 0817081602 1915041708 22191823230807

(b). Vignere cipher using key: SUNSHINE

(i) graphical method:

Plaintext: ENEMY PLANE SPOTTED

Ciphertext: WHREF XYEFY FHVBGIV

(ii) numerical method: 2308180506 2425050625 06082202070922

1. Decrypt the following cipher text using the Vigene table, and key: HANGZHOU

Plaintext: IEGZDYZUAEGNZUBYCEE

Ciphertext: PETFCFNOHETTYBPSJER

1. Decrypt the following ciphertext which was encrypted using rail fence cipher with key =3.

Plaintext: EVERYDAYISANEWDAY

Ciphertext: EYIEYVRDYSNWAEAAD

1. Encrypt the following using the rail fence cipher with key=4

Plaintext: THERE IS NO SUCH THING AS A FREE LUNCH

Ciphertext: TISHSECHSUTIARENHEEOCNAFURNHG L

1. \*We received the following ciphertext which was encoded with a shift cipher:

xultpaajcxitltlxaarpjhtiwtgxktghidhipxciwtvgtpilpitghlxiwiwtxgqadds

* 1. Perform an attack against the cipher based on a letter frequency count: How many letters do you have to identify through a frequency count to recover the key? What is the cleartext?

Shift key: 15

Cleartext: if we all unite we will cause the rivers to stain the great waters with their blood

* 1. Who wrote this message?