Graphical user interface, application

Description automatically generatedGraphical user interface, application, Word

Description automatically generated

* 1. Equipment theft threatens the confidentiality, availability, and integrity of computer systems and data.
  2. Unauthorised copying of software threatens the copyright of the software and its associated intellectual property, as well as the availability of the software.
  3. Modification of existing files threatens the integrity of the files and the data stored therein.
  4. Destroying messages threatens the confidentiality, availability, and integrity of the messages and any data contained therein.
  5. Observing traffic patterns of messages threatens the confidentiality and privacy of the messages, as well as the availability of the data contained therein.

1. Source 2 is more random on average. This is because the sum of the squared probability values for Source 2 (0.09 + 0.01 + 0.25 + 0.01 = 0.36) is greater than the sum of the squared probability values for Source 1 (0.09 + 0.04 + 0.16 + 0.01 = 0.30). This indicates that Source 2 has a more unpredictable distribution, making it more random on average.
2. A binary source with two events only has a maximum entropy of 1 bit. When plotted on a graph of entropy against binary probability distribution, the graph will be a straight line with a slope of -1, with the entropy decreasing as the probability of the event increases.

Graphical user interface, application, Word

Description automatically generatedTable

Description automatically generated with low confidence

Pros:

-The cryptosystem does not require a key exchange and is based on a one-time keypad, making it secure.

-It is computationally efficient and does not require a large amount of resources.

Cons:

-The system is vulnerable to a man-in-the-middle attack.

-Alice and Bob must be online at the same time in order to exchange messages.

John's cryptosystem does work, as it provides a secure way for Alice and Bob to communicate. By using the one-time keypad and the XOR operation, Alice and Bob are able to send and receive messages in a secure manner. The one-time keypad ensures that the same key cannot be used more than once, which makes it difficult for an attacker to break the encryption. Additionally, since no key exchange is required, Alice and Bob can communicate without having to worry about sharing a key. John's cryptosystem is secure, but it is vulnerable to man-in-the-middle attacks and requires Alice and Bob to be online at the same time, making it less than ideal for secure communication.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Alice |  | Charlie |  | Bob |
| m |  |  |  |  |
| ↓ |  |  |  |  |
| Encrypt(m) | **→** | **Encrypt(Encrypt(m))** | **→** | **Decrypt(Encrypt(Encrypt(m)))** |
|  |  |  |  | **↓** |
| Decrypt(Decrypt(Encrypt(Encrypt(m)))) | **←** | **Encrypt(m)** | **←** | **Decrypt(Encrypt(m))** |
| ↓ |  | **↓** |  |  |
| Encrypt(m) |  | **Encrypt(m)** |  |  |
| ↓ |  |  |  |  |
| Encrypt(Encrypt(m)) | **→** | **Encrypt(Encrypt(Encrypt(m)))** | **→** | **Decrypt(Encrypt(Encrypt(Encrypt(m))))** |
|  |  | **↓** |  | **↓** |
|  |  | **Encrypt(m)** |  | **Encrypt(m)** |