What is Plaintext? (Examples, Plaintext Attack, Is It a Lapse in Security?)

Cyber Security | Anti Virus | Safe & Security

What is Plaintext?

In cryptography, Plaintext is usually plain readable text before it is encrypted into ciphertext or readable text after it is decrypted. Any message, document, file, or the like that is not meant to be encrypted is referred to as plaintext.

- The input to a cryptosystem is plaintext, and the output is ciphertext. Algorithms in cryptography convert plaintext to ciphertext and ciphertext to plaintext.
- Plaintext saved in a computer file must be protected since its contents are completely disclosed and hence potentially actionable if it is stolen, disclosed, or sent without permission. If data is to be saved, the storage medium, device, components, and backups must all be protected.

Plaintext vs. Ciphertext: What is the Difference?

Plaintext and ciphertext are like water and ice in that they can be transformed back and forth without affecting the inherent composition of the usable form. **Clear text**, on the other hand, is not always the same as plaintext.

Because binary files are not human-readable, they are not considered plaintext, yet they are still accessible to end-users. The following are some examples of non-plaintext binary files –

- Application files that can be executed;
- Files with rich media, such as photos, videos, and audio recordings; and
- Data files created by applications such as spreadsheets, databases, and word processors, which may be stored partially or entirely as binary data.

Examples of Plaintext

Plaintext is recommended in most applications. Plaintext should be shown in a browser, word processor, or email client, for example. However, early Internet network protocols occasionally transmitted user ID and password combinations in plaintext. This is a bad

security practice since it exposes user credentials for systems that are accessible remotely over a public network such as the Internet.

- Although the Password Authentication System provided a two-way handshake authentication exchange protocol, it did not include a mechanism for encrypting credentials.
- Those credentials are exposed if plaintext passwords are written in application configuration files. Developers that keep plaintext passwords in their source code are less likely to expose their credentials.
- Password protection in PowerShell scripts to avoid revealing those passwords in their scripts, developers must take care.

Plaintext – Is It a Lapse in Security?

Plaintext handling that isn't secure can expose flaws in a cryptosystem by allowing an attacker to bypass the cryptography entirely. Plaintext, whether in electronic or paper format, is vulnerable in use and storage.

If plaintext is saved in a computer file, the storage medium, the machine and its components, as well as all backups, must all be safe. When sensitive data is processed on computers with detachable mass storage, the physical protection of the removed disk is critical.

While securing a computer, useful (as opposed to handwaving) security must be both physical (e.g., against burglary, brazen removal under the guise of supposed repair, installation of covert monitoring devices, etc.) and virtual (e.g., brazen removal under the guise of supposed repair, against identity theft, installation of covert monitoring devices, etc).

Modern cryptographic systems are resistant to known-plaintext or even chosen-plaintext assaults, therefore they may not be completely compromised. Older systems used fewer effective techniques like padding and Russian copulation to disguise information in plaintext that may be easily guessed to combat the consequences of plaintext data loss on security.

Plaintext Attack

The **known-plaintext attack (KPA)** is a cryptanalysis attack paradigm in which the attacker has both the plaintext (also known as a crib) and its encrypted form (ciphertext). These can be used to uncover more secrets, such as secret keys and codebooks.

Known-plaintext attacks are common against traditional ciphers. A Caesar cipher, for example, can be decrypted entirely using a single letter of corresponding plaintext and

ciphertext. If there are less than 26 unique pairs, a universal monoalphabetic substitution cipher requires multiple character pairs and some guessing.