Permanent Privacy Encryption Overview

TECHNICAL WHITEPAPER

Content

Introduction

Permanent Privacy Encryption uses "Advanced Encryption Standard (AES) 256-bit as a foundation with an expansion on the decryption space (patent-protected).

- The decryption space contains every single readable character, words of any language and all potential combinations.
- When a 'try-them-all' (brute-force) method is used to attack pp-Encryption, the decryption results will contain every readable sentence up to the length of the original message.
- This feature is what makes pp-Encryption truly unhackable since it is mathematically impossible to find the original message.

In other words, PP-Encryption can be considered an enhanced AES encryption method to the point where its security strength reaches an "unhackable" level by achieving "Perfect Security" as defined and created by Claude Shannon.

Passwords and Control File

PP-Encryption uses two passwords and one control file as an input for both encryption and decryption.

The passwords used in PP-Encryption are usual AES (256 bit) passwords in the AES environment. Note that the 256-bit AES method requires the length of its password to be a maximum of 32 8-bit characters.

The control file is an arbitrary random file and the content include both printable and non-printable characters of any language and any combinations of them. This control file will be incorporated into the AES environment as an entity.

For PP-Encryption, the length of the control file is required to be longer than the original message to satisfy the Shannon Perfect Security requirement.

The passwords and control file can be considered a "Password Space" forcing the expansion of the AES encryption and decryption spaces via a space expansion.

Blending Module Forcing AES Expansion

The design of PP-Encryption includes a blending module which embeds the passwords, control file and AES into a single encryption/decryption entity with the following characteristics:

- Keep the basic AES style, structures and environment
- Maintain the accuracy of the internal bit-stream flow within PP-Encryption.
- Force the expansion of the AES passwords, encryption, and decryption spaces.
- Ensuring successful encryption and decryption.

PP-Encryption forces a series of space expansions on the traditional AES encryption method.

The design of the blending module also makes sure that there is minimum computational cost for the space expansion than normal encryption and decryption usage.

The expansion has a big impact when PP-Encryption is under brute-force attack by making the brute-force attack completely powerless.

Expansion of Decryption Space

The blending module in the previous section forces the PP-Encryption entity to expand the decryption space.

Therefore, the decryption space of PP-Encryption will contain every single readable character, words of any language and all potential combinations of them.

In other words, when a ‘try-them-all’ (brute force) attack is attempted on pp-Encryption, the decryption results will contain every readable sentence up to the length of the original message. This feature makes pp-Encryption truly unhackable.

For example, if you encrypt a four letter word 'East', the brute force attack will have 'Home', 'Time', 'West', 'Note' and any four character words as well as your original word 'East'. Therefore there is no mathematical chance for a hacker to identify your original text.

Unhackable Feature

The design of PP-Encryption includes a "Search Module" to make sure that the decryption of the Brute-force attack will cover and "Pre-Define" the readable message up to the length of the original message.

This situation is explained with the following example:

Given a PP-Encryption encrypted message (or cipher text) such as:

0a a3 b3 f2 1b 42 00 13 7f 7c 0d b2 fc c1 b0 47 d0

b8 b4 b7 78 1e 81 34 11 d6 fe da 2e a9 9a 2b 62 28

7e 20 b3 70 16 e4

The original message is (with the proper passwords and control file):

"Meet Me At 2pm Tomorrow"

For the same encrypted text, the search module will allow you to pre-set a fixed text such as:

"Kill KyK In One Month"

and produce a piece of binary control file e.g. "zFile01.bin" so that the PP-Decryption will product the text "Kill KyK In One Month" as a decryption result.

For the same encryption text and another control file "zFile02.bin", it will produce the decryption result "Abort All EA Operations".

With another control file "zFile03.bin", it can produce the decryption result "Enemy Will Attack Today.

Conclusion

Blending modules, space expansion and the search module can be applied to most encryption methods. PP-Encryption can be interpreted as a big expansion on the AES-Decryption- Space; providing unhackable security to its users.

The pp-Encryption Engine uses the "Advanced Encryption Standard" (AES) as a foundation with an expansion on decryption space/Cipher Space (patent-protected). Therefore, the decryption space will contain every single readable character, words of any language and all combinations of them.

In other words, when there is a try-them-all (brute force) attack on pp- Encryption, the decryption results will contain every readable sentence up to the length of the original message. This feature makes pp-Encryption truly unhackable.

For example, if you encrypt a four letter word 'East', the brute force attack will have 'Home', 'Time', 'West', 'Note' as well as your original word 'East'.

There is no chance for the hacker to identify your original text.

For more information, see “Watch it in action” Video.