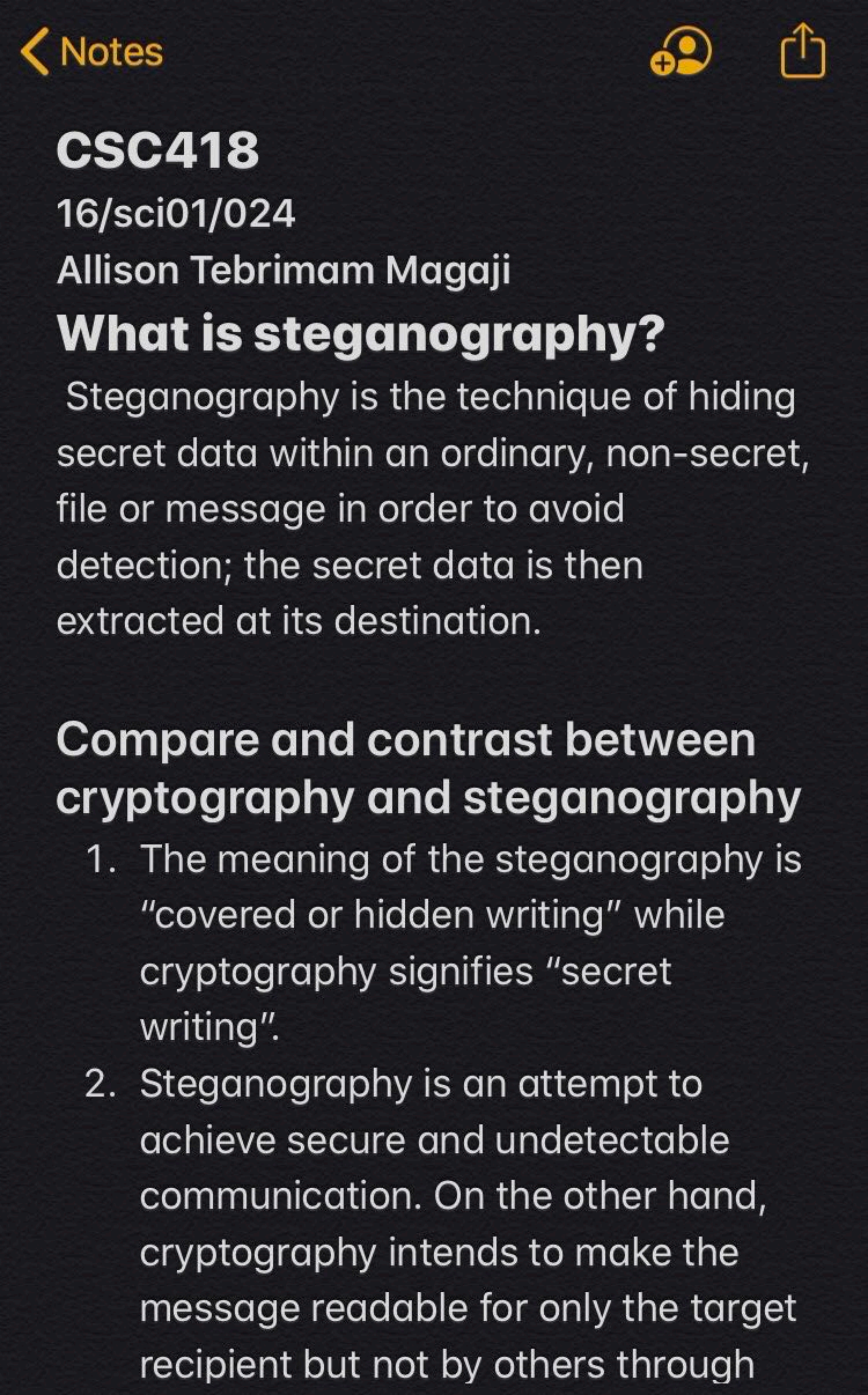


CSC418

16/sci01/024

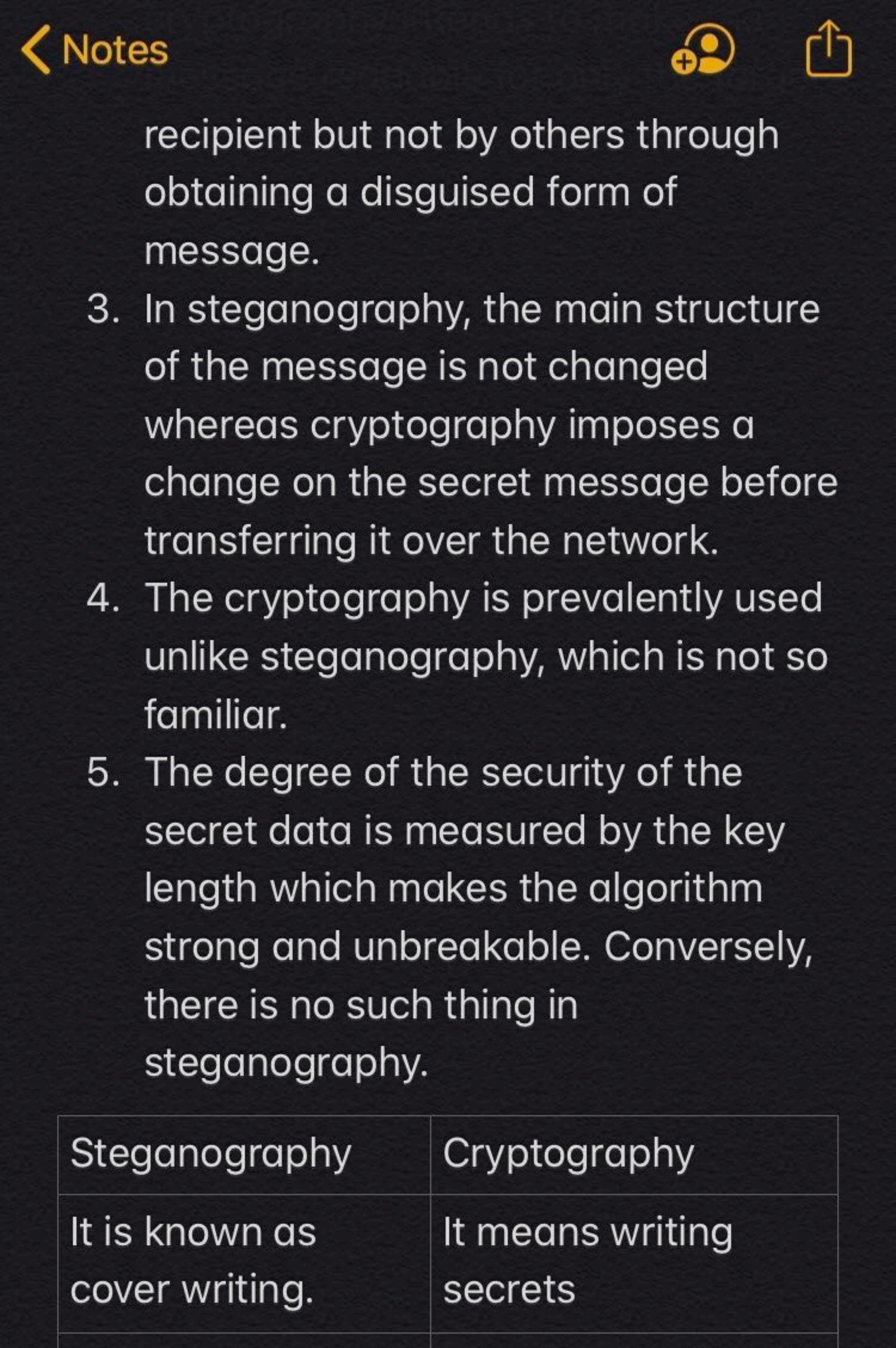
Allison Tebrimam Magaji

What is steganography?

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.

Compare and contrast between cryptography and steganography

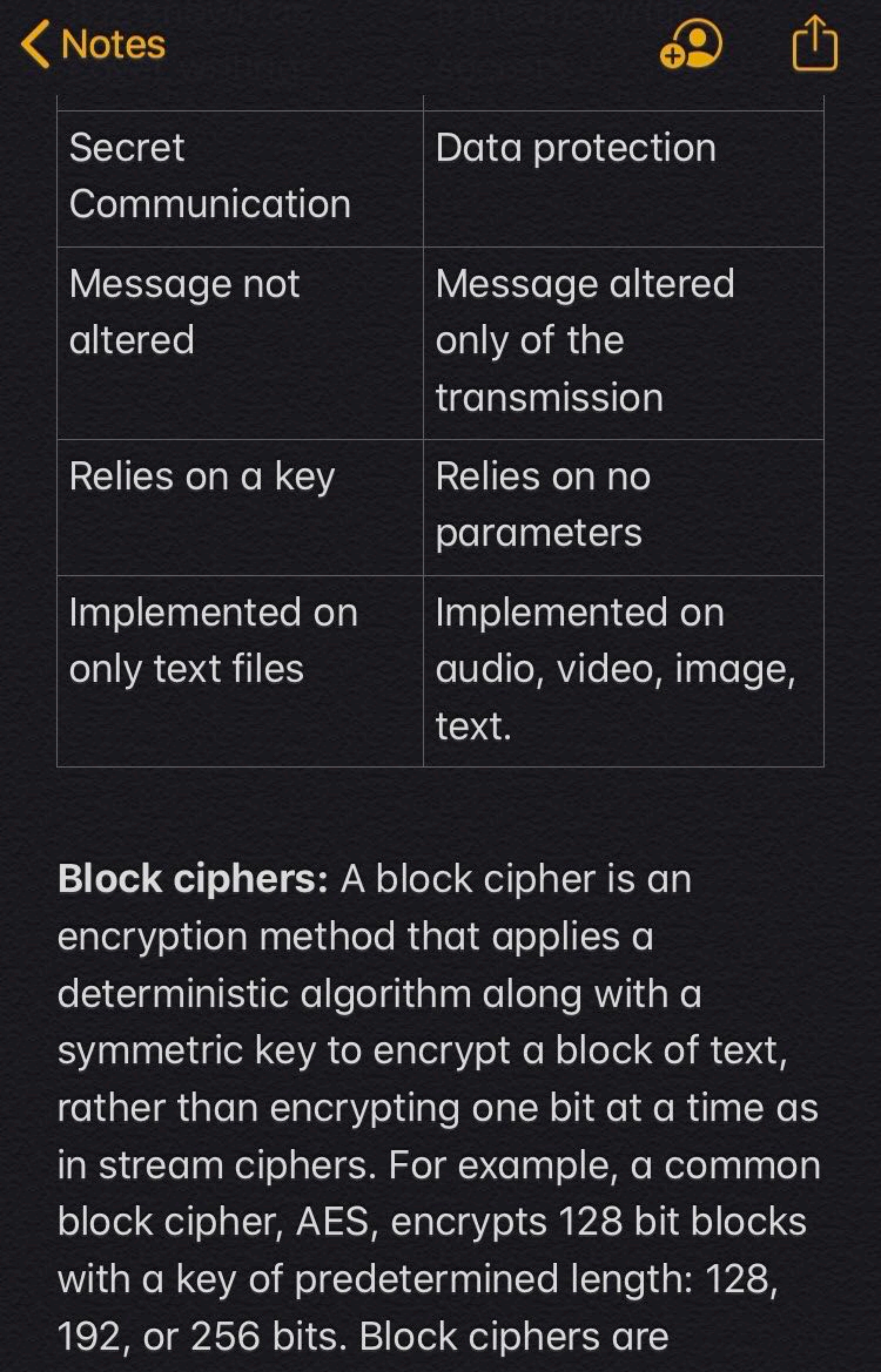
1. The meaning of the steganography is "covered or hidden writing" while cryptography signifies "secret writing".
2. Steganography is an attempt to achieve secure and undetectable communication. On the other hand, cryptography intends to make the message readable for only the target recipient but not by others through



recipient but not by others through obtaining a disguised form of message.

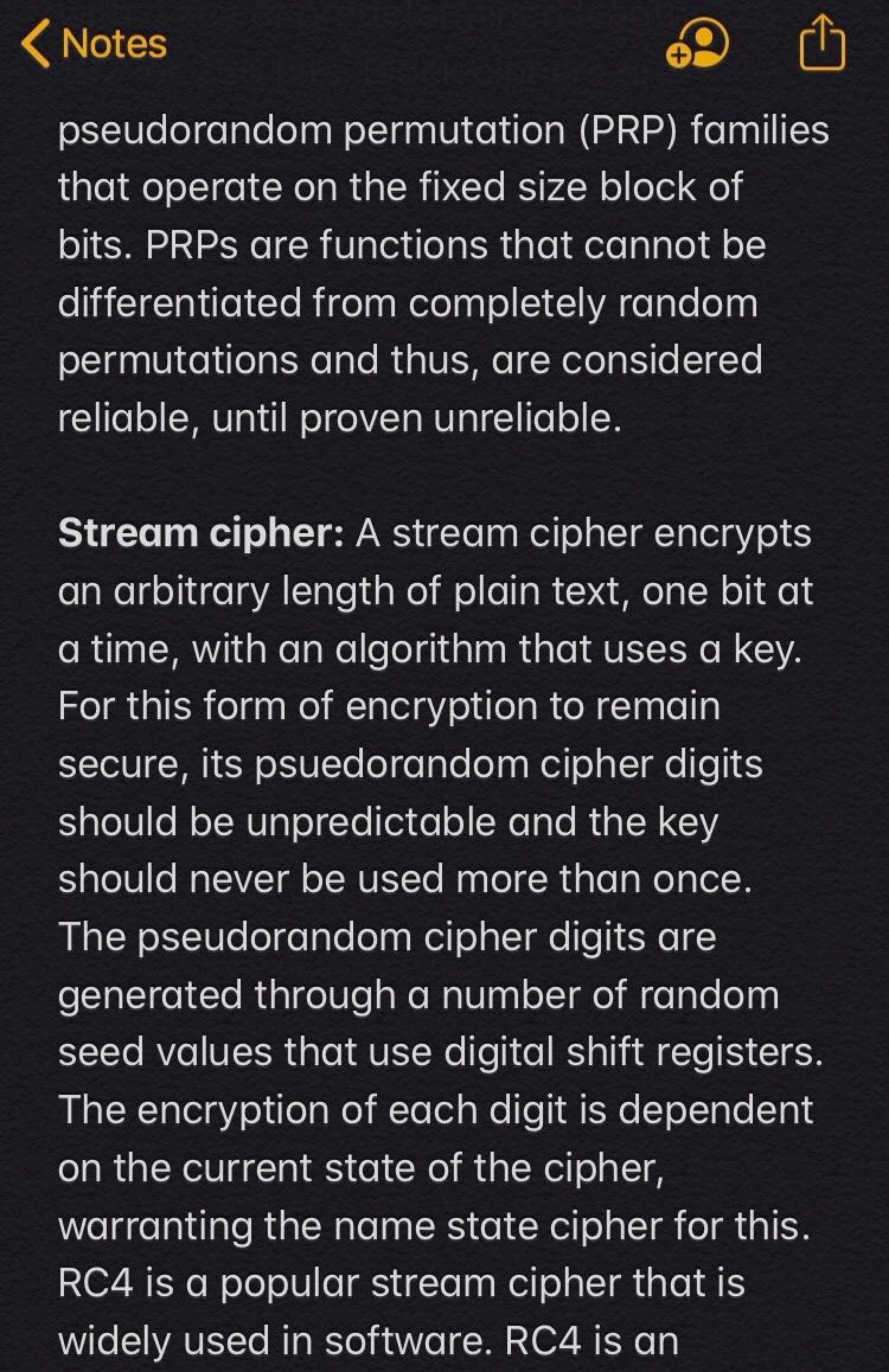
3. In steganography, the main structure of the message is not changed whereas cryptography imposes a change on the secret message before transferring it over the network.
4. The cryptography is prevalently used unlike steganography, which is not so familiar.
5. The degree of the security of the secret data is measured by the key length which makes the algorithm strong and unbreakable. Conversely, there is no such thing in steganography.

Steganography	Cryptography
It is known as cover writing.	It means writing secrets



Secret Communication	Data protection
Message not altered	Message altered only of the transmission
Relies on a key	Relies on no parameters
Implemented on only text files	Implemented on audio, video, image, text.

Block ciphers: A block cipher is an encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time as in stream ciphers. For example, a common block cipher, AES, encrypts 128 bit blocks with a key of predetermined length: 128, 192, or 256 bits. Block ciphers are



pseudorandom permutation (PRP) families that operate on the fixed size block of bits. PRPs are functions that cannot be differentiated from completely random permutations and thus, are considered reliable, until proven unreliable.

Stream cipher: A stream cipher encrypts an arbitrary length of plain text, one bit at a time, with an algorithm that uses a key. For this form of encryption to remain secure, its psuedorandom cipher digits should be unpredictable and the key should never be used more than once. The pseudorandom cipher digits are generated through a number of random seed values that use digital shift registers. The encryption of each digit is dependent on the current state of the cipher, warranting the name state cipher for this. RC4 is a popular stream cipher that is widely used in software. RC4 is an widely used in software. RC4 is an example of a modern symmetric-key stream cipher. ... RC2, RC5, and RC6 are symmetric-key block ciphers. RC4 does not generate its keystream by using a LFSR. For RC4, stream combinations are done on byte-length strings of plaintext.