A Review Paper on Cryptography

A small summary of the paper is as below:

Cryptography is something that is widely used to ensure the confidentiality of data. It's a way to hide data from the people who shouldn't see the message without the receiver. Cryptography is now one of the most important methods for data communication and preserving security.

Digital Data communication means how data is transferred and received in the form of a digital bitstream or other similar ways. Here, Data security is a big issue. If an attacker or hacker can know what is being sent or received, the vulnerabilities and costs are enormous. So, there should be a secure system where security will be ensured.

A hash function is any function that can be used to map data of arbitrary size to fixed-size values. The values returned by a hash function are called hash values, hash codes, or simply hashes.

Properties of Hash Function:

1. Non-reversibility, or one-way function.
2. A change in just one bit of the original password should result in a change to half the bits of its hash. In other words, when a password is changed slightly, the output of enciphered text should change significantly and unpredictably.
3. Determinism.
4. Collision resistance. It should be hard to find two different passwords that hash to the same enciphered text.
5. Non-predictable. The hash value should not be predictable from the password.

Block Cipher and Stream Cipher belong to the symmetric key cipher. These two block ciphers and stream cipher are the methods used for converting the plain text into ciphertext.

The main difference between a Block cipher and a Stream cipher is that a block cipher converts the plain text into cipher text by taking the plain text's block at a time. While stream cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.

Digital Signatures Algorithm is a FIPS (Federal Information Processing Standard) for digital signatures. It was proposed in 1991 and globally standardized in 1994 by the National Institute of Standards and Technology (NIST).

Requirements of Digital Signature might be:

01. Ability to generate their own Signature on their Documents

02. Every user has to have the ability to recognize and verify their own Digital Signature if needed later.
03. Most importantly, Only the owner should have the ability to generate the signature for their documents only by the owner.