The above are the equations for CFB encryption mode. The following are the definitions for the symbols

LSB - Least Significant Bit
IV - Initialization Vector
C - Cipher Text
$P_i$ - Plain Text
E(K,$I_i$) - Initialization Vector is encrypted with Key K.
$S_r(X_i)$ - Most Significant r bits of $X_i$

# 2 Cryptographic Hashing And Digital Signatures

## 2.1 Cryptographic Hashing

Alice finds an algorithm and publishes only the digest of the algorithm in a newspaper, 15 years later when the algorithm is to be discovered again, can she convince the judge that the algorithm was already discovered 15 years ago by her is the question.

**No,Alice cannot prove to the judge that she was the one who found it 15 years ago**.The explanation goes as such.

A cryptographic hash function is a hash function which takes an input (or 'message') and returns a fixed-size alphanumeric string. The string is called the 'hash value' or the 'message digest'.

The ideal hash function has three main properties:

1)It is extremely easy to calculate a hash for any given data.
2)It is extremely difficult to calculate an alphanumeric text that has a given hash that is Hashing is irreversible.
3)It is extremely unlikely that two slightly different messages will have the same hash that is Hashing is unique enough but not entirely unique.

What Alice cannot prove here is that she is the one has published the hash in the newspaper.A third party member can claim that they were the one who published it having a different input that maps to the same hash value although this is extremely and computationally difficult.

This kind of a attack on Hashing is called as the **Collision Resistance Attack.**A good hashing algorithm should be hard to find two different inputs that output to the same hash value that is, two inputs a and b such that
H(a) = H(b) but a not equal to b.

Finding such an input pair that maps to the same hash value is extremely difficult.Every hash function with more inputs than outputs will necessarily have collisions.Consider SHA-256 that produces 256 bits of output from a large input. Since it must generate one of $2^{256}$ outputs for each member it is clear that some inputs will hash to the same output. **Collision resistance does not mean that no collisions exist but they are hard to find.There have been incidents where hashing Algorithm MD5 has been broken.A 2013 attack by Xie Tao, Fanbao Liu, and Dengguo Feng breaks MD5 collision resistance in $2^{18}$ time. This attack runs in less than a second on a regular computer.**

The birthday paradox also supports this that if a hash function produces N bits of output the attacker need to compute only $2^{N/2}$ hash operations for random input and he is supposed to find a matching input. Hence to conclude this problem, Alice **cannot justify** that she was the one who published the digest in the newspaper as a third party member might claim it with a different input although it takes $2^{128}$(in case if the hashing algorithm is SHA-256) computations to find a input that outputs to the same hash value.

## 2.2 Digital Signatures

Can Alice prove if a Digital Signature was released instead of a Hash?

**Yes, Alice can prove if a Digital Signature was released instead of a Hash.** A digital signature is a mathematical technique used to validate the authenticity and integrity of a message.Digital Signatures are based on public-key cryptography such as RSA where we generate a public and a private key.The general working of a digital signature is that when a signer electronically signs a document, the signature is created using the signer's private key, which is always securely kept by the signer.Then a hash is created by the signing algorithm and encrypting that hash. The resulting encrypted hash is the digital signature. The signature is also marked with the time that the document was signed. If the document changes after signing, the digital signature is invalidated.

Consider Alice has released a digital signature(encrypted hash in a journal) that was encrypted with her private key. After 15 years, alice can prove that she was the one who found it because only she can decrypt it using her public key. No other third party can decrypt because their public key cannot decrypt the hash and hence Alice **can justify** to the judge that she was the one who found it 15 years ago. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves computaional time.