ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORTIHM

By
Ananya Sajwan

CSE3501 – Information Security Analysis and Audit
VIT Chennai

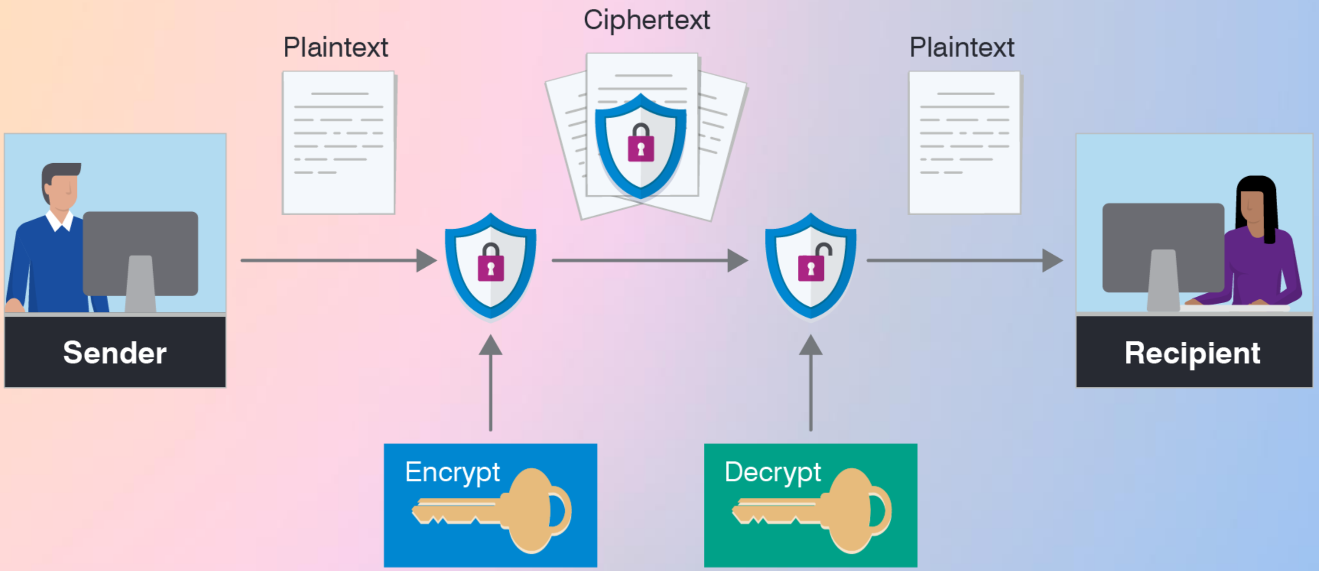
ENCRYPTION-DECRYPTION IN INFORMATION SECURITY

- In the fields of information security and cryptography, encryption is the process of encoding a message or information in a way that only authorized parties can access it and those who are not authorized cannot.

Different Encryption standards:

- Data Encryption Standard (now obsolete)
- Advanced Encryption Standard
- RSA (the original public-key algorithm)
- Open PGP

How does encryption work?



Different keys are used to encrypt and decrypt messages

ENCRYPTION ALGORITHMS

- **Triple DES Encryption -** Though it is slowly being phased out, Triple DES is still a dependable hardware encryption solution for financial services and other industries.
- **RSA Encryption -** RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet.
- **Advanced Encryption Standards (AES) -** The Advanced Encryption Standard (AES) is the algorithm trusted as the standard by the U.S. government and many other organizations. AES is considered resistant to all attacks, with the exception of brute-force attacks.

Twofish encryption algorithm

Blowfish encryption algorithm

IDEA encryption algorithm

MD5 encryption algorithm

HMAC encryption algorithm

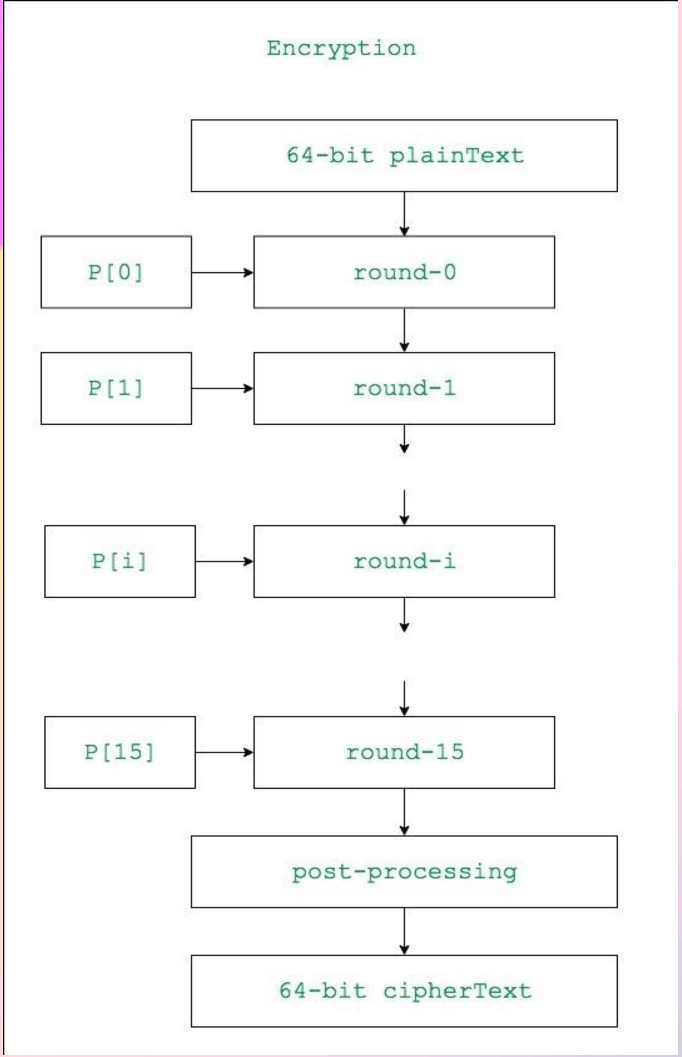
BLOWFISH ENCRYPTION ALGORITHM

Blowfish is an encryption technique designed by Bruce Schneier in 1993 as an alternative to DES Encryption Technique.

It is significantly faster than DES and provides a good encryption rate.

It is one of the first, secure block ciphers not subject to any patents and hence freely available for anyone to use.

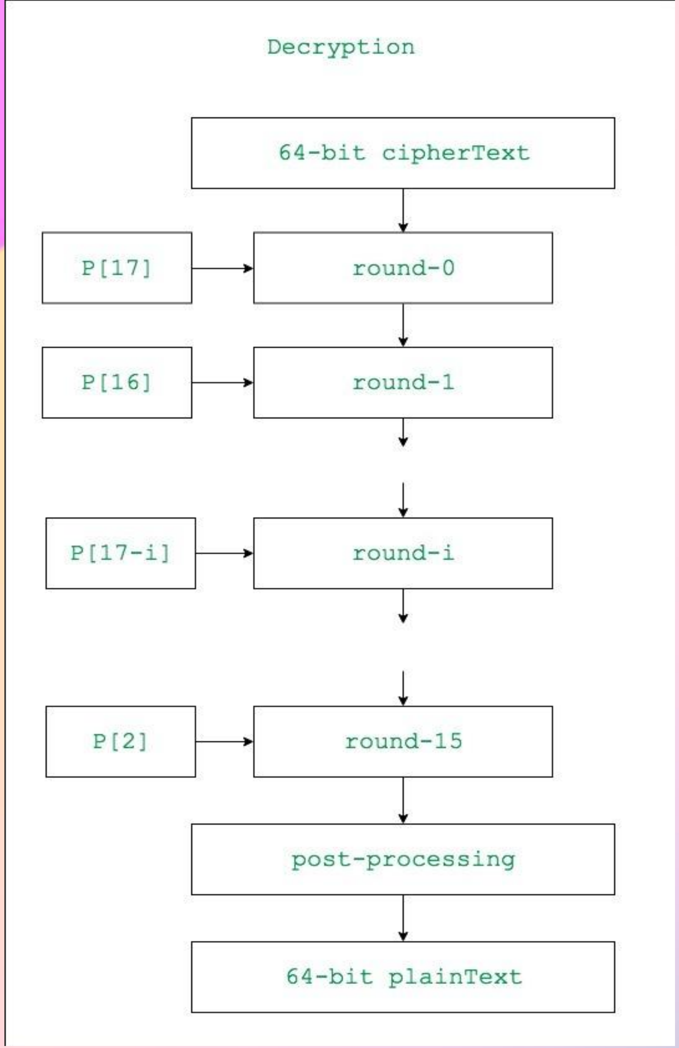
Block Size: 64-bits
Key Size: 32-bits to 448-bits variable size
number of subkeys: 18 [P-array]
number of rounds: 16
number of substitution boxes: 4 [each having 512 entries of 32-bits each]



The entire encryption process can be elaborated using this flowchart.

There are mainly

- **Step1: Generation of subkeys**
- **Step2: initialise Substitution Boxes**
- **Step3: Encryption:** The encryption function consists of two parts: **Rounds** and **Post-processing**



The entire decryption process can be elaborated using this flowchart.

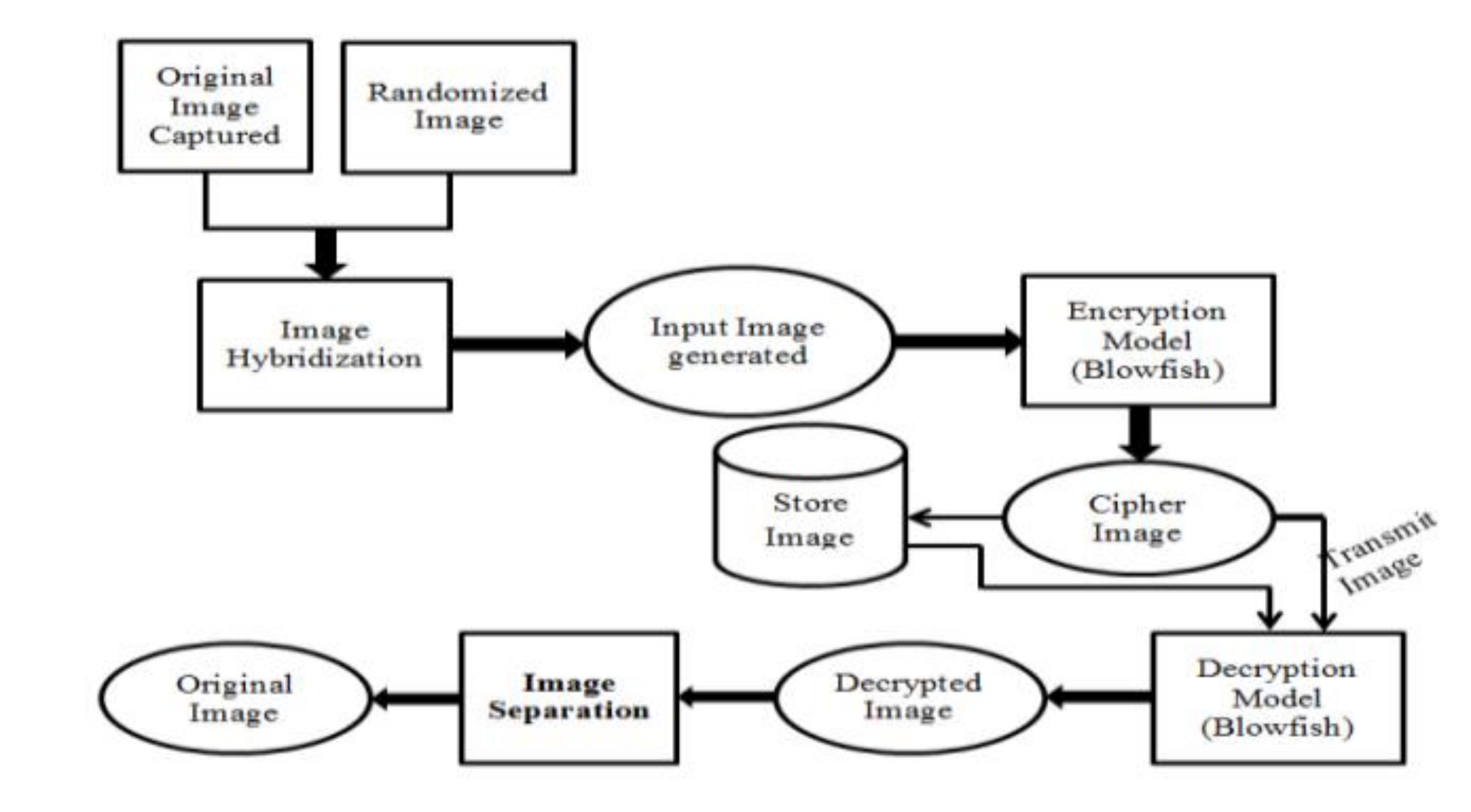
There are mainly

- **Step1: Generation of subkeys**
- **Step2: Initialise Substitution Boxes**
- **Step3: Decryption:** The decryption function consists of two parts: **Rounds** and **Post-processing**

APPLICATIONS OF BLOWFISH ALGORITHM

- File and Disk Encryption software like CryptoForge, CryptoDisk etc. use Blowfish Algorithm.
- The algorithm is also used in password management tools like 1Password, KeyRing Mini, PasswordsPlus etc. to encrypt and store passwords.
- It is also used by various email encryption software like Alock, SecuMail, Cypherus and Z1 SecureMail Gateway.
- Blowfish Algorithm has also been used in many recent research papers to develop enhanced image encryption technologies.

Image Encryption using Blowfish Algorithm



BEST PRACTICES FOR ENCRYPTION

1. **Know the laws:** When it comes to safeguarding the personal information, organizations must adhere to many overlapping, privacy-related regulations. The top six regulations that impact many organizations include: FERPA, HIPAA, HITECH, COPPA, etc.
2. **Assess the data:** Entities should perform a data risk assessment and implement encryption if the evaluation indicates that encryption would be a “reasonable and appropriate” safeguard.
3. **Determine the required or needed level of encryption**
4. **Be mindful of sensitive data transfers and remote access:** Communicating or sending data over the internet needs Transport Layer Security (TLS), a protocol for transmitting data over a network, and AES encryption.
5. **Note the fine print details:** Regulatory compliance entails much more than simply password-protecting an office’s workstations. It requires using encryption to protect data-at-rest when stored on school systems or removable media device.

CONCLUSION

Encryption and Decryption are important aspects of all organizations for 4 main reasons-

- **Authentication**
- **Privacy**
- **Regulatory Compliance**
- **Security**

Data encryption is a common and effective security method—a sound choice for protecting an organization's information. In a world where cybercrimes are on the rise, it's comforting to know that there are as many methods available to protect network security. The real challenge is deciding which techniques an internet security expert should employ that best suits their organization's specific situation.