I. INTRODUCTION

A. Cryptography

Cryptography is the study of knowledge concealment and verification. It includes the protocols, algorithms and techniques to firmly and systematically stop or delay unauthorized access to information. Cryptography comes from the Greek words Cryptós, "hidden", and graphy "to write" - or "hidden writing". People that study and develop cryptography are referred to as cryptographers. The study of avoiding the employment of cryptography for unintended recipients is termed science, or code breaking. Cryptography and cryptanalysis are grouped together under the umbrella term cryptology, encompassing the whole subject. In follow, "cryptography" is referred as field as whole, particularly as associate branch of knowledge. Cryptography is associate knowledge base subject, drawing from many fields. Before the time of computers, it had been closely associated with linguistics. Today the stress has shifted, and cryptography made a depth use of technical areas of arithmetic, particularly those areas together referred to as distinct arithmetic. This includes topics from variety theory, scientific theory, process complexity, statistics and combinatorial. It’s conjointly a branch of engineering, however associate uncommon one because it should contend with active, intelligent and malevolent opposition.

B. Encryption

In cryptography the method of encryption messages or information is done in such a way that solely licensed parties will browse it.[1] cryptography doesn't itself stop interception, however denies the message content to the fighter.[2] In associate cryptography theme, the message or information, brought up as plaintext, is encrypted, generating cipher text which will solely be browse after decrypted.[2] For technical reasons, associate cryptography theme typically uses a pseudo-random cryptography key generated by associate algorithmic program. It's in essence to decipher the message while not possessing the key, but for a well-designed cryptography theme, massive machine resources and talent area unit needed. Associate authorized recipient will simply decipher the message with the key, provided by the mastermind to recipients however to not unauthorized interceptors.

C. Encryption and Decryption:

- **Encryption:** a process of encoding a message so that it's meaning is not obvious.
- **Decryption:** the reverse process.

Cryptography system can classify into two systems, symmetric and asymmetric. Encryption standards classification was done based on the key. Symmetric Encryption standard uses same key (i.e Private Key) for both Encryption and Decryption. Asymmetric Encryption standard uses two keys, one for Encryption and different key for Decryption procedure.

![Cryptography Diagram](image)

**Fig1. Cryptography.**

D. The Need for Cryptography

Security often requires that data to be kept safe from unauthorized access. And the best line of defense is physical security (placing the machine to be protected behind physical walls). However, physical security is not always an option (due to cost and/or efficiency considerations). Instead, most computers are interconnected with each other openly, thereby exposing them and the communication...
channels that they use. This problem can be broken down into five requirements that must be addressed:

1. Confidentiality: assuring that private data remains private.
2. Authentication: assuring the identity of all parties attempting access.
3. Authorization: assuring that a certain party attempting to perform a function has the permissions to do so.
4. Data Integrity: assuring that an object is not altered illegally.
5. Non-Reputation: assuring against a party denying a data or a communication that was initiated by them.

II. LITERATURE SURVEY

A. AES

The Advanced Encryption Standard (AES) is an encryption algorithm for securing information in commercial transactions in the private sector. AES is a symmetric key encryption standard adopted by the U.S. government. The Advanced Encryption Standard consists of three block ciphers. They are: AES-128, AES-192, and AES-256. Each of the above standard ciphers is 128-bit block size with key sizes of 128, and 192 & 256 bits respectively. AES is based on a substitution-permutation network, in which the input data (also called "plaintext") and the cryptographic key are successively processed by substitution boxes (S-boxes) or permutation boxes (P-boxes), in mathematical operations. The 128-bit input block is divided into a 4x4 array of 8 bits (one byte) each, called the "State." The S-boxes effectively substitute one 8-bit number for another and were designed in such a manner that a change in one bit at the input changes at least half of the output bits, known as the "avalanche property." In contrast, the P-boxes permute, or shuffle, the 8 input bits to produce an 8-bit output. The mathematical operations of the S-boxes and P-boxes are organized in a number of successive "rounds." Each round in AES is comprised of four transformations, or operations. These are called "SubBytes," "ShiftRows," "MixColumns," and "AddRoundKey." All bytes in AES, including the key, are considered to be finite field elements, not numbers, for purposes of the mathematical operations within these transformations.

Specifically, the finite field in AES is defined as a Galois field of size $2^8$, with $2^{8^6}$ elements. FIPS 197 specifies the mathematical details of AES implementation. Each round takes two inputs: the previous State and a Round Key. The Round Key is derived from the cryptographic key according to the Rijndael key schedule as defined in FIPS 197. There are a variable number of rounds according to the AES key length: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. The final round omits the MixColumns transformation; otherwise all of the rounds perform the same four transformations. The result of the State after the final AES round is "ciphertext," which bears no resemblance to the plaintext. Decryption of the ciphertext is the inverse of the encryption steps, using the same symmetric key used for encryption. Encryption and Decryption are highly important security steps nowadays.

Now there are file and data encryption software are available as well. Data encryption is the mechanism of converting a message (plain text) into some other text (called ciphertext) so that readers can't understand the original message; however some authorized party can understand that ciphertext using the method called Decryption which converts the ciphertext into original message. As many software applications store sensitive personal data in databases, encryption has become a must. Ideally nobody (including the software developers) should not be able to view these user specific real data. RIJNDAEL algorithm developed to replace the unsafe DES and the low 3DES. The 56 bits DES algorithm developed by IBM has encountered enormous threats obtained from the ordinary computers. In view of this, American National Standards and Technology Association issued the official notice to seek for the next generation encryption standard (AES). The Advanced Encryption Standard (AES) is the current encryption standard intended to be used It is also becoming a global standard for encryption or other security features. It has been designed to have very strong resistance against the classical approximation attacks. since Rijndael is very algebraic, new algebraic attacks appeared.

![AES Flow Diagram](image-url)
III. PROPOSED BLOWFISH ALGORITHM

In cryptography, Blowfish is a keyed, symmetric block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. While no effective cryptanalysis of blowfish has been found to date. Schneier designed Blowfish as a general-purpose algorithm, intended as a replacement for the aging DES and free of the problems associated with other algorithms. At the time, many other designs were proprietary, encumbered by patents or kept as government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public domain, and can be freely used by anyone." Notable features of the design include key-dependent S-boxes and a highly complex key schedule.

A. Blowfish Algorithm

Blowfish is a variable-length key, 64-bit block cipher. The algorithm consists of two parts: a key-expansion part and a data-encryption part. Key expansion converts a key of at most 448 bits into several sub-key arrays totaling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key-dependent permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

![Blowfish Flow Diagram](image)

**Fig3. Blowfish Flow Diagram.**

B. Sub-keys

Blowfish uses a large number of sub-keys. These keys must be precomputed before any data encryption or decryption.

1. The P-array consists of 18 32-bit sub-keys: P1, P2, ..., P18.
2. There are four 32-bit S-boxes with 256 entries each:
   - S1,0, S1,1, ..., S1,255
   - S2,0, S2,1, ..., S2,255
   - S3,0, S3,1, ..., S3,255
   - S4,0, S4,1, ..., S4,255

The exact method used to calculate these sub-keys will be described later.

C. Encryption and Decryption

Blowfish is a Feistel network consisting of 16 rounds (Fig3). The input is a 64-bit data element, x.

1. Fig Blowfish Algorithm Fiestel Network.

Divide x into two 32-bit halves: xL, xR
For i = 1 to 16:
   - xL = xL XOR Pi
   - xR = F(xL) XOR xR
Swap xL and xR
Swap xL and xR (Undo the last swap.)
   - xR = xR XOR P17
   - xL = xL XOR P18
Recombine xL and xR

2. Function F:

![F Network](image)

**Fig4. F Network.**

Divide xL into four eight-bit quarters: a, b, c, and d
F(xL) = ((S1,a + S2,b mod 232) XOR S3,c) + S4,d mod 232

Decryption is exactly the same as encryption, except that P1, P2, ..., P18 are used in the reverse order. Implementations of Blowfish that require the fastest speeds should unroll the loop and ensure that all sub-keys are stored in cache.

3. Implementation:

The Field Programmable Gate Array is majorly used for generation ASIC IC’s to the computations. They offer more speed in execution process. SO, for generation ASIC IC’s FPGA’s are majorly used. The AES and Blow Fish algorithms are simulated and synthesized on Xilinx ISE using FPGA configuration tabulated below.
A. Usha Kiran, Mohd Javeed Mehd

Table 1: Configuration of FPGA

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Family</td>
<td>Spartan 3</td>
</tr>
<tr>
<td>Device</td>
<td>XC3S4000</td>
</tr>
<tr>
<td>Package</td>
<td>fg1156</td>
</tr>
<tr>
<td>Speed Grade</td>
<td>-4</td>
</tr>
</tbody>
</table>

Memory Comparison in Bytes occupied by AES and Blowfish

Fig 5. Memory Comparison.

The below graph shows the timing analysis of both AES and Blowfish algorithm in ns

Fig 6. Delay comparisons.

V. REFERENCES