CHAPTER – 5

MULTIPHASE ENCRYPTION: AN EXTENSION OF MULTIPLE ENCRYPTION

5.1 MULTIPHASE ENCRYPTION

The proposed model of multiphase encryption is the extension of the multiple encryption. In the multiphase encryption technique, multiple encryption using different encryption algorithms is treated as a single phase. In the proposed technique, multiple phases of such multiple encryption are integrated into a singular unit, which enhances the data security in enormous amount.

The proposed motives of encryption techniques provide better security in comparison of multiple encryption because in this technique number of multiple encryptions are used with highly secure different encryption algorithms. The multiphase encryption comprises a number of phases in which number of multiple encryptions are embedded in such a manner that the complexity of a cryptosystem is increased in large extent. As we know that the complexity of encryption algorithm is directly proportional to the security of the algorithm, the security of this cryptosystem is enhanced multiple times.

5.2 WORKING PRINCIPLE OF PROPOSED TECHNIQUE OF MULTIPHASE ENCRYPTION

In the proposed technique of multiphase encryption, number of encryption phases are involved. Each encryption phase is equivalent to the proposed model of multiple encryption where data is encrypted multiple times with different and modern encryption algorithms.

In the proposed model of multiphase encryption, each phase follows the proposed model of multiple encryption where data is encrypted by highly secure encryption algorithms such as AES, Serpent, Twofish and RC6. The result of the first phase is treated as an input for the second phase, where this input is further encrypted by AES, Serpent, Twofish and RC6 encryption.
algorithms. The result of the second phase is considered as an input for third phase and this process is continued until we reach at the desired level of security for the crucial data.

The working criteria of the proposed technique of multiphase encryption are illustrated in following figure.

![Operational Architecture of Each Phase of Multiphase Encryption](image)

**Fig. 5.1 Operational Architecture of Each Phase of Multiphase Encryption**

Where,

C1 = Ciphertext of First Encryption

C2 = Ciphertext of Second Encryption
C3 = Ciphertext of Third Encryption

C4 = Ciphertext of Fourth Encryption

Where,

P = Original Message or Plaintext of Multiphase Encryption

C = Final Ciphertext of Multiphase Encryption

Fig. 5.2 Operational Architecture of Multiphase Encryption
C_1 = Ciphertext of Phase 1

C_2 = Ciphertext of Phase 2

C_{N-1} = Ciphertext of Phase (N-1)

5.3 AN ALGORITHM FOR MULTIPHASE ENCRYPTION

The algorithm for the proposed technique of multiphase encryption can be described in following manner:

(1) Take an original message or plaintext as an input for multiphase encryption.

(2) In each phase of multiphase encryption, perform the following operations:

   (a) Perform the encryption process using AES algorithm

   (b) Perform the encryption process on the ciphertext of AES algorithm using a Serpent encryption algorithm

   (c) Perform the encryption process on the ciphertext of Serpent algorithm using the Twofish algorithm

   (d) Perform the encryption process on the ciphertext of the Twofish algorithm using RC6 encryption algorithm

   (e) Store the result of RC6 encryption algorithm as the output or ciphertext of phase 1 and forward it to the next phase

(3) Repeat step 2 until the desired level of security and final ciphertext of last phase should be considered as an output or ciphertext of multiphase encryption.

5.4 INTERNAL ARCHITECTURE OF MULTIPHASE ENCRYPTION

The internal architecture of multiphase encryption can be described as a layered architecture of multiple phases. In each phase of multiphase encryption, the internal architecture of various secure encryption algorithms as AES, Serpent, Twofish and RC6 are integrated.
A) AES Algorithm and its Architecture

<table>
<thead>
<tr>
<th>Description of AES Encryption Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designers</td>
</tr>
<tr>
<td>First Published</td>
</tr>
<tr>
<td>Structure</td>
</tr>
</tbody>
</table>

**Best Public Cryptanalysis**

- **Brute-force attack**: Due to the key length of 128, 192 or 256 bits, a brute-force attack is not possible
- **Analytical attacks**: There is no analytical attack known that is better than brute-force
- **Side-channel attacks**: Several side-channel attacks have been published
  (Side-channel attacks do not attack the underlying algorithm but the implementation of it.)

Table 5.1: Brief Description of AES Encryption

![Substitution-Permutation Structure](image-url)

**Fig. 5.3: Substitution-Permutation Structure**
Fig. 5.4: Internal Architecture of AES Algorithm
B) Serpent Algorithm and its Architecture

<table>
<thead>
<tr>
<th>Description of Serpent Encryption Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designers</td>
</tr>
<tr>
<td>First Published</td>
</tr>
<tr>
<td>Structure</td>
</tr>
</tbody>
</table>

**Best Public Cryptanalysis**

- All known attacks are computationally infeasible. A 2011 attack breaks 11 round Serpent (all key sizes) with $2^{116}$ known plaintexts, $2^{107.5}$ time and $2^{104}$ memory.

- The same paper also describes two attacks which break 12 rounds of Serpent-256. The first requires $2^{118}$ known plaintexts, $2^{228.8}$ time and $2^{228}$ memory. The other attack requires $2^{116}$ known plaintexts and $2^{121}$ memory but also requires $2^{237.5}$ time.

**Table 5.2: Brief Description of Serpent Encryption**

![Internal Architecture of Serpent Algorithm](image.png)
C) Twofish Algorithm and its Architecture

<table>
<thead>
<tr>
<th>Designers</th>
<th>Bruce Schneier</th>
<th>Key Size (Bits)</th>
<th>128, 192, 256</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Published</td>
<td>1998</td>
<td>Block Size (Bits)</td>
<td>128</td>
</tr>
<tr>
<td>Structure</td>
<td>Feistel Network</td>
<td>No. of Rounds</td>
<td>16</td>
</tr>
</tbody>
</table>

Best Public Cryptanalysis

- Truncated differential cryptanalysis requiring roughly 251 chosen plaintexts.
- An impossible differential attack that breaks 6 rounds out of 16 of the 256-bit key version using 2256 steps.

Table 5.3: Brief Description of Twofish Encryption

![Diagram of Twofish Algorithm]

Fig. 5.6: Internal Architecture of Twofish Algorithm
D) RC6 Algorithm and its Architecture

<table>
<thead>
<tr>
<th>Designers</th>
<th>Key Size (Bits)</th>
<th>First Published</th>
<th>Block Size (Bits)</th>
<th>Structure</th>
<th>No. of Rounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ron Rivest, Matt Robshaw, Ray Sidney, Yiqun Lisa Yin</td>
<td>128, 192, 256</td>
<td>1998</td>
<td>128</td>
<td>Feistel Network</td>
<td>20</td>
</tr>
</tbody>
</table>

**Description of RC6 Encryption Algorithm**

<table>
<thead>
<tr>
<th>Designers</th>
<th>Key Size (Bits)</th>
<th>First Published</th>
<th>Block Size (Bits)</th>
<th>Structure</th>
<th>No. of Rounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ron Rivest, Matt Robshaw, Ray Sidney, Yiqun Lisa Yin</td>
<td>128, 192, 256</td>
<td>1998</td>
<td>128</td>
<td>Feistel Network</td>
<td>20</td>
</tr>
</tbody>
</table>

**Best Public Cryptanalysis**

Our analysis demonstrates that RC6 is highly resistant to differential and linear cryptanalytic attack, which are currently the two most effective analytical attacks on block ciphers.

**Table 5.4: Brief Description of RC6 Encryption**

![Fig. 5.7: Internal Architecture of RC6 Algorithm](image-url)
5.5 AN ENCRYPTION TOOL USED FOR PROPOSED MULTIPLE AND MULTIPHASE ENCRYPTION TECHNIQUE

Symmetric Cipher Online Tool permits to encrypt and decrypt the arbitrary message using various secure and advanced encryption algorithms as Triple DES, AES, Serpent, Blowfish, Twofish and RC4 etc. Symmetric ciphers use the same key for encryption and decryption purpose. These ciphers are easily computable and able to process the large message in real time effectively. Symmetric ciphers are convenient due to use of a single entity as the encryption key for the encryption and decryption of crucial data. Symmetric ciphers using secure and advance encryption algorithm provide adequate security for confidential data due to a number of complex operations.

Fig. 5.8: Symmetric Ciphers Online Encryption Tool

In this tool, an additional variable into the operational function that contributes in holding the state of calculation because it is required to generate different encrypted blocks when two
identical blocks are encrypted with same functions and same key. The state is changed during encryption and decryption process when this additional variable is combined with the content of each block. The initialization value of this additional variable is called initialization vector. The initialization or state vector is combined with the input block to change the vector state.

**Usage of Symmetric Cipher Online Tool**

In this tool, we select the input type as a text string or a file. In case of text string, enter the input into the input text box. Otherwise, press the "Browse" button to upload the input file. Now, select the cryptographic algorithm we want to use in Function field. On the basis of the selected cryptographic algorithm, the initialization vector (IV) field is shown or hidden. The initialization vector is always represented by a sequence of bytes in hexadecimal form.

**AES – Symmetric Ciphers Online**

![Encryption Tool Interface]

Fig. 5.9: Selection of Input Mode in Encryption Tool

The operation mode should be selected in the Mode field and enter an encryption key in the Key field. The permitted key length varies for particular cryptographic algorithms, which can be seen in following list. For some cryptographic algorithm, when the encryption key is changed, a key function is automatically filled in the initialization vector field.
Finally, click on the "Encrypt" button or "Decrypt" button as per the requirement of encryption and decryption of input text. The autodetect feature detects the input text and can turn OFF by changing the current type of input under Input text field.

The output data are displayed in the hexadecimal form and also can be downloaded in a binary file.

**Limitations**

In this tool, the maximum size of input text string is 1,31,072 characters and maximum size of input file is 2,097,151 bytes. In online mode, a specific usage limit in a day is permitted for one IP address.
5.6 THE IMPLEMENTATION OF MULTIPHASE ENCRYPTION USING ENCRYPTION TOOL

The implementation of proposed multiple and multiphase encryption is done through advance encryption tool. In this implementation, we analyzed the results of various encryption techniques of each phase in Multiphase Encryption. In each phase, the input text is encrypted by AES, Serpent, Twofish and RC4/RC6 encryption algorithm. Here, we can see clearly that security is enhanced due to multiple encryption with the original data in each phase of Multiphase Encryption.

A) AES Encryption

In live implementation of AES Encryption, we input the original message or plaintext and we observed the following results.

**AES – Symmetric Ciphers Online**

![AES Encryption Using Encryption Tool](image)

**Fig. 5.11: AES Encryption Using Encryption Tool**
B) Serpent Encryption

Second encryption is performed using a Serpent encryption algorithm, where the output or ciphertext of AES is given as input to the Serpent algorithm. The following results are observed.

**Serpent – Symmetric Ciphers Online**

![Encryption Tool](image)

Input type: Text

Input text:

<table>
<thead>
<tr>
<th>Text</th>
<th>c7</th>
<th>bd</th>
<th>08</th>
<th>e0</th>
<th>3e</th>
<th>5d</th>
</tr>
</thead>
<tbody>
<tr>
<td>44</td>
<td>e0</td>
<td>c7</td>
<td>bd</td>
<td>08</td>
<td>e0</td>
<td>3e</td>
</tr>
<tr>
<td>2f</td>
<td>43</td>
<td>de</td>
<td>a4</td>
<td>1f</td>
<td>c3</td>
<td>a8</td>
</tr>
<tr>
<td>13</td>
<td>55</td>
<td>05</td>
<td>5a</td>
<td>94</td>
<td>b5</td>
<td>0d</td>
</tr>
<tr>
<td>56</td>
<td>9e</td>
<td>0c</td>
<td>a1</td>
<td>2d</td>
<td>56</td>
<td>db</td>
</tr>
<tr>
<td>9e</td>
<td>8e</td>
<td>c6</td>
<td>09</td>
<td>bb</td>
<td>e3</td>
<td>39</td>
</tr>
</tbody>
</table>

Function: SERPENT

Mode: CBC (cipher block chaining)

Key: RESEARCH

Init. vector: c8 73 bc c6 c3 19 61 d6 99 60 f9 9d d7 db 9f

**Fig. 5.12: Serpent Encryption Using Encryption Tool**
C) Twofish Encryption

Third encryption is performed using a Twofish encryption algorithm, where the output or ciphertext of the Serpent is given as input to the Twofish algorithm. The following results are observed.

**Twofish – Symmetric Ciphers Online**

---

**Input type:** Text

**Input text:**

<table>
<thead>
<tr>
<th>a</th>
<th>o</th>
<th>b</th>
<th>l</th>
<th>i</th>
<th>u</th>
<th>y</th>
</tr>
</thead>
<tbody>
<tr>
<td>h</td>
<td>s</td>
<td>e</td>
<td>m</td>
<td>a</td>
<td>g</td>
<td>z</td>
</tr>
<tr>
<td>I</td>
<td>}</td>
<td>D</td>
<td>m</td>
<td>D</td>
<td>g</td>
<td>z</td>
</tr>
</tbody>
</table>

- **Function:** TWOFISH
- **Mode:** CEC (cipher block chaining)
- **Key:** RESEARCH
- **Init. vector:** c873 bc c8 c3 19 61 d6 99 b0 9d 95 d7 db 9f

![Twofish Encryption Using Encryption Tool]

Fig. 5.13: Twofish Encryption Using Encryption Tool
D) RC4/RC6 Encryption

Third encryption is performed using a RC4/RC6 encryption algorithm, where the output or ciphertext of the Twofish is given as input to the RC4/RC6 algorithm. The following results are observed. The ciphertext of RC4/RC6 algorithm is considered as final ciphertext for a particular phase of multiphase encryption.

### RC4 – Symmetric Ciphers Online

<table>
<thead>
<tr>
<th>Input type:</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input text:</td>
<td>(plain)</td>
</tr>
<tr>
<td>Function:</td>
<td>RC4 (ARCFOUR)</td>
</tr>
<tr>
<td>Mode:</td>
<td>Stream</td>
</tr>
<tr>
<td>Key:</td>
<td>RESEARCH</td>
</tr>
</tbody>
</table>

![Encryption Tool](image_url)

**Fig. 5.14: RC4/6 Encryption Using Encryption Tool**
So, we have seen that in the above mentioned phase of multiphase encryption, the data is encrypted through secure and advanced multiple encryption to provide more data protection. The implementation results of multiphase encryption can be illustrated in the following way.

1) Encryption Process in each phase of Multiphase Encryption

\[
\text{Plaintext}
\]

("Research is creating new knowledge.")

<table>
<thead>
<tr>
<th>AES Encryption</th>
<th>Serpent Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plaintext</strong></td>
<td><strong>Encrypted text</strong></td>
</tr>
<tr>
<td>(&quot;Research is creating new knowledge.&quot;)</td>
<td>encrypted data</td>
</tr>
</tbody>
</table>

**Encrypted text:**

- AES Encryption: 00000000 84 ed c7 bd 69 a8 3e 5d 2f 43 de a4 1f c3 a8 92
- Serpent Encryption: 0000010 13 6b 05 5a 94 b5 d0 13 55 9e 0c a1 2d 96 db 10
- [Download as a binary file] [Show more] [Show all]
Chapter 5: Multiphase Encryption: An Extension of Multiple Encryption

2014

Designing Some Multiple and Multiphase Encryption Techniques for the Enhancement of Data Security

Fig. 5.15: Implementation Results of Multiphase Encryption
Chapter-5: Multiphase Encryption: An Extension of Multiple Encryption

1) Decryption Process in each phase of Multiphase Encryption

In each phase of multiphase encryption, decryption process takes place in reverse order as it is done in the encryption process.
Designing Some Multiple and Multiphase Encryption Techniques for the Enhancement of Data Security

This process of encryption or decryption should be repeated in each phase of multiphase encryption to make the process more and more complex. In such a way, we can achieve high...
level security for highly confidential data specially for military information, credit card information and social security number.

5.7 EXPERIMENTAL RESULTS AND ANALYSIS

As we mentioned earlier that we can categorize the encryption algorithms on the basis of its ability to secure the confidential data against security attacks and its processing speed.

The performance of proposed model of multiphase encryption is calculated and compared with proposed multiple encryption model in table 5.5.

<table>
<thead>
<tr>
<th>Factors</th>
<th>Triple DES</th>
<th>Proposed Multiple Encryption (First Phase)</th>
<th>Second Phase</th>
<th>Proposed Multiphase Encryption (N Phases)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Size</td>
<td>64 Bits</td>
<td>128 Bits</td>
<td>128 Bits</td>
<td>128 Bits</td>
</tr>
<tr>
<td>Cipher Type</td>
<td>Symmetric Cipher</td>
<td>Symmetric Cipher</td>
<td>Symmetric Cipher</td>
<td>Symmetric Cipher</td>
</tr>
<tr>
<td>Key Length</td>
<td>112 Bits</td>
<td>512 Bits</td>
<td>1024 Bits</td>
<td>512×N Bits</td>
</tr>
<tr>
<td>Cryptanalysis</td>
<td>Strong against Differential</td>
<td>Strong against Differential</td>
<td>Strong against Differential</td>
<td>Strong against Differential</td>
</tr>
<tr>
<td>Security</td>
<td>Considered Not Secure</td>
<td>Considered Highly Secure</td>
<td>Considered Highly Secure</td>
<td>Considered Extremely Highly Secure</td>
</tr>
<tr>
<td>Possible Combinations</td>
<td>$2^{112}$</td>
<td>$2^{512}$</td>
<td>$2^{1024}$</td>
<td>$2^{512\times N}$</td>
</tr>
<tr>
<td>Time to Crack All Possible Keys</td>
<td>800 Days</td>
<td>4.08×10^{18} Yrs.</td>
<td>8.16×10^{18} Yrs.</td>
<td>4.08×N×10^{18} Yrs.</td>
</tr>
</tbody>
</table>

Table 5.5: Performance Comparison of Proposed Model of Multiphase Encryption

As per analysis of experimental results, we found that proposed model of multiphase encryption is generating better performance in comparison of proposed and existing multiple encryption algorithms due to following reasons.
1) It supports large size of data blocks as 128, 192 and 256 bits.

2) It is supposed to exhibit extremely high level security due to very large key length.

3) It is supposed to provide strongest security against differential attacks.

4) It is considered as extremely high secured encryption algorithm due to multi-level encryption.

5) It requires checking of huge number of possible combinations to guess the correct key.

6) It is computationally highly secure against brute force attack because lot of time is required to check all possible keys.

5.8 BENEFITS AND LIMITATIONS OF PROPOSED MULTIPLE AND MULTIPHASE ENCRYPTION

Multiphase Encryption provides better security than multiple encryption over the vulnerable wireless network as the internet. Multiphase Encryption has various benefits in the area of data security, which can be described in following manner.

- Multiphase encryption provides better security because if even some encryption algorithms are recognized or some of the secret keys are broken the confidentiality of the original message can still be maintained.

- It provides a multilayer architecture as per the international standards of network security.

- It provides high level security to protect sensitive information.

- It enables the industry or organization to flow at a normal pace silently securing crucial data in the background.

- It provides solid and multilayer protection in the event of a security breach.

- It provides effective and efficient multiple key management scheme through secure and advanced encryption algorithms.

- It establishes the secure multiple key exchange mechanism.
It provides additional security layers over multiple encryption.

It provides multilayer security for highly confidential information such as credit card information, social security number and military information.

It addresses security related regulatory compliance issues.

Multiphase Encryption has some limitations which can be described as:

It is quite complex due to its complex architecture.

It increases the system overhead.

It requires more memory to save various components of multiple encryption.

It consumes more time to encrypt and decrypt the multiple phases.

It requires additional implementation cost due to repeated