International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 05 | May - 2021 ISSN: 2582-3930

Rim Hybrid Cipher Design Model for Encryption in Cryptography

Rishika Subhash Desai , Prof. Kirti Wanjale

Computer Engineering Department
Vishwakarma Institute of Information Technology

Abstract -In this paper, one unique way of enhancing the security strength of the combination of block and stream cipher has been discussed. This is achieved with the help of a parameter, known as 'RIM' that improvises the design. The overall functionality is slightly varied from the usual working of a hybrid cipher. We have used multiple assumptions while portraying the functioning of the design. However, once achieved, it can become a significant parameter that contributes to the overall strength of encryption.

Key Words:encryption, cryptography, hybrid cipher, design model, quantum key distribution, block cipher, stream cipher

1. INTRODUCTION

Combining stream and block ciphers to introduce a hybrid cipher is a technique well known and accepted for more than a decade.However, additional encouragement towards the security part can be done by introducing a parameter (here, named as 'rim') with the key. RIM stands for 'Random Input Method'.

2. Body of Paper

Harris[i] mentions in his paper that combining stream and block ciphers in different mixing patterns can eliminate the risk of theoretical vulnerabilities and known attack vectors. Various combinations of design implementations can make the attacks utterly worthless and significantly more problematic.

A few set of assumptions that we are going to consider to focus on the design structure effectively are as follows:
1. The secret key between the two parties communicating over a channel is already known.
2. The communication channel is secure for the rim transfer.
3. The algorithms used to encrypt the data are computationally challenging to crack due to their complexity.
4. The sequence of the encryption is labelled and well known beforehand. The only task that remains is to apply rim methodology here.
5. The data going through the block cipher should be less than or equal to the input bits required to encrypt.

MIXING PATTERN

'RIM' is essentially a number that provides three features to design our encryption process.
Firstly, a Rim will decide the number of divisions of the stream cipher output. It'll then answer the number of block ciphers to be implemented after stream cipher encryption. Secondly, it provides the buffer content characters between outputs of two block ciphers. Lastly, itwill decide thenumber of rounds, after which there shall be a predefined shuffling pattern to change the block cipher algorithms.

Since we have already assumed that the sequence of encryption is known, the Rim uses the distribution of the result generated from the stream cipher first. Let's assume two famous characters, Alice and Bob, which use encryption algorithm models to communicate. The sequence of steps is described below as follows:
1.Since the keys of algorithms and a predefined pattern are known between Alice and Bob, Alice will send a Rim 'm' to Bob. This Rim is essentially a value.
2. Depending on the Rim number, the systems will determine the number of block cipher algorithms to be chosen, the number of buffer characters, and the time limit to shuffle the block cipher algorithms.
3. Once the system is all set and Alice is ready to send the message over the secure channel, the data is encrypted using the stream cipher algorithm. It generates E1.
4. This E1 is now divided into m number of sections, and each section goes through a unique block cipher algorithm in a parallel fashion. The outputs shall be E11, E12, E13, and so on.
5. Between each generated output of the m block ciphers; there shall be a m dummy buffer.
6. This overall generates encrypted data, let's calls it $E_{overall}$, traverses through the secure channel and thus, reaches Bob.
7. Now, consider after m (Rim number), such rounds, the system will pause the encryption process for some time and then shuffle the block cipher algorithms. This is assumed that the shuffling pattern is necessarily the same in both the machines over which Alice and Bob are encrypting/decrypting the data.
8.Since the stream cipher remains the same, one cycle can be considered complete only when the message length bits are less than or equal to all the combined required input bits of the block cipher.
9.So until the last bit of the last cycle of the Rim count is not sent from Alice's side and not received at Bob's end, the Rim cycle shall not change.
10.Unless all the shuffling mechanisms are done, and the machine reaches the initial stage of algorithmic pattern, the machine should not request the user to send another Rim. This can only happen when Alice or Bob voluntarily want to request a Rim change.

Example:A and B, between the two parties, want to communicate over the secure channel using the Rim model. A sends out the Rim value to be 3.
Rim=3 implies three block ciphers, three dummy characters, and three cycles of encryption before shuffling.
Assuming the stream cipher is S1, the three predefined block ciphers are B1, B2, and B3. Once the system is set and ready to send a message, A shall send 12 bits of data to B.

During the encryption process, this message is passed over S1 to generate the encrypted text E1.

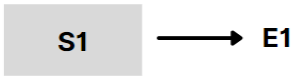

Figure 1: Stream cipher encryption

For further block cipher rounds, E1 is divided into three parts of 4 bits each. Let's name them E11, E12, and E13.

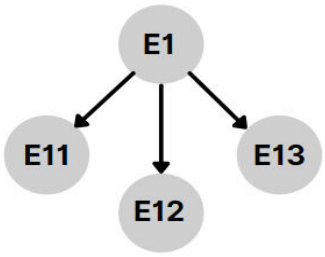

Figure 2: Distribution of encrypted data depending on the Rim

These three bits of data pass through B1, B2, and B3, generating E (E11), E (E12), and E (E13), respectively.

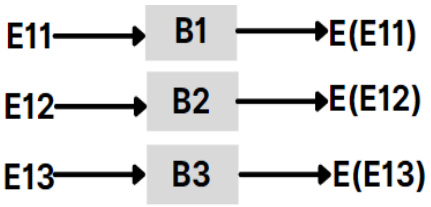

Figure 3: Parallel Block cipher method (One cycle of Rim)

However, before sending this data over the secure channel, we need to insert the buffer characters. Thus,

Eoverall= E(E11)+dummy+E(E12)+dummy+E(E13)+dummy

This is the output for one cycle of the encryption model using Rim. Now that the last cycle is completed, there is a shuffling of the algorithms between B1, B2, and B3.

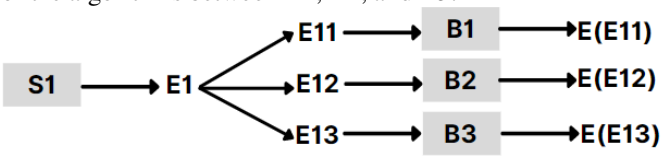

Figure 4: One cycle of Rim

As per the assumptions, the length of input bits by the sender should not exceed the combined length of all the inputs of the block ciphers. However, if this happens, the message can be put into buffer memory to store until the first cycle with input length equals to the combined block is completed.

Assume the capacity of the block cipher is fixed to be 10 bits each (can be variable) and Rim=3. So the input value for the first round of encryption should not be more than 30 bits.

However, if it does exceed this margin, then the system shall move the result of additional bits of stream cipher to the buffer memory, where it waits until the first cycle is completed. Here, the process will create a small percentage of latency. However, these are hypothetical numeric values that we have assumed. The final implementation of the model shall be much larger than this.

IMPORTANCE OF RIM

Most of the paper deals with the concept of introducing an additional parameter called Rim, but it should also answer why. The Rim improves the complexity of cracking the encrypted data. The person having to crack the entire design system and know the plain text needs to know two elements: the Rim and the secret key.

In the worst-case scenario, let's assume that the Rim is known (however, we shall also see other ways to strengthen this model in the next section). The following predefined shuffling pattern between the two machines should remain unknown to the perpetrator. He must try all the possible combinations of the Rim to get the plaintext, and brute-forcing will be, in this case, the most exhaustive option here.

As Harris discusses in his paper, out of three perpetrators- Tom, Dick, and Harry, the scholar Harry have fair chances to crack and get near to knowing this pattern, given that he has all the resources to seek knowledge about the structure.

Given that the value of Rim increases over the levels, the complexity of the algorithm shall increase, and the hypothetical threat actors will find it significantly challenging to crack. Nevertheless, the user will always have an option to change the Rim value if they suspect an intrusion during communication.

FUTURE SCOPE

To make this encryption model immune to attacks, one can introduce the concept of Quantum Key Distribution (QKD) by J.Aditya[ii] to share the Rim. Assuming that the Rim was not shared over secure communication, then QKD can use photons over polarized mediums to share the value. This serves the purpose of secure transmission and intrusion detection. As after knowing the Rim value, the model will merely remain a combination of a hybrid cipher. Thus, proactive steps must be taken to ensure that the value isn't disclosed even before the transmission has started.

Another method through which the system can stay secure is replacing the different set of algorithms after each cycle. This method can result in strengthened security of the design model. However, I won't propose changing all the algorithms playing a part here without estimating the cost of implementation approximately. Thus, changing one algorithm in a fixed or random order at the end of every cycle after shuffling is one way to improve complexity.

These two approaches concentrate on combining techniques but can also be expensive at the same time. However, they can effectively cater for the thought experiment and bring out enhanced immunity from attack vectors.

3. CONCLUSIONS

With the inclusion of the Rim parameter in the model of hybrid cipher, I thus conclude that it can make noteworthy changes in the security aspect of encryptions. Assuming the algorithms are chosen can be challenging or straightforward, the complexity of the model and various versions of varying intricacy can be achieved.
Out of different design algorithms of the hybrid cipher, the Rim model shall supplement the existing reliability and dependability.

ACKNOWLEDGEMENT

I acknowledge that this work of mine is based on my own self-study and reference papers I used to propose a research.

REFERENCES

1. Sandy H: Exploring Cipherspace: Combining stream ciphers and block ciphers: IACR Cryptol. ePrint Arch. 2008: 473 (2008).
2. J. Aditya, P. Shankar Rao. Proceedings of Computer Society of India (CSI). February 2005

BIOGRAPHIES

My name is Rishika Desai. I'm a cybersecurity researcher trying to explore various domains and its potential influences in shaping the security strengths of users. I therefore, intend to propose various such implementation ideas that can be beneficial for the society.