A Report on Industrial Training – II

For

Research Trainee at SAG Lab (Analysis of Block Ciphers)
9 weeks

Prepared By: -
Kunal Manik
4th Year CSE-B
10314210074

Submitted To: -
Ms. Pallavi Agarwal
Assistant Professor
SRM University Delhi-NCR Campus, Sonepat

Under the Expert Guidance of
Dr. Dhananjoy Dey
Scientist
DRDO – SAG Lab, Metcalfe House

SRM UNIVERSITY, DELHI-NCR, SONEPAT
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Bonafide Certificate

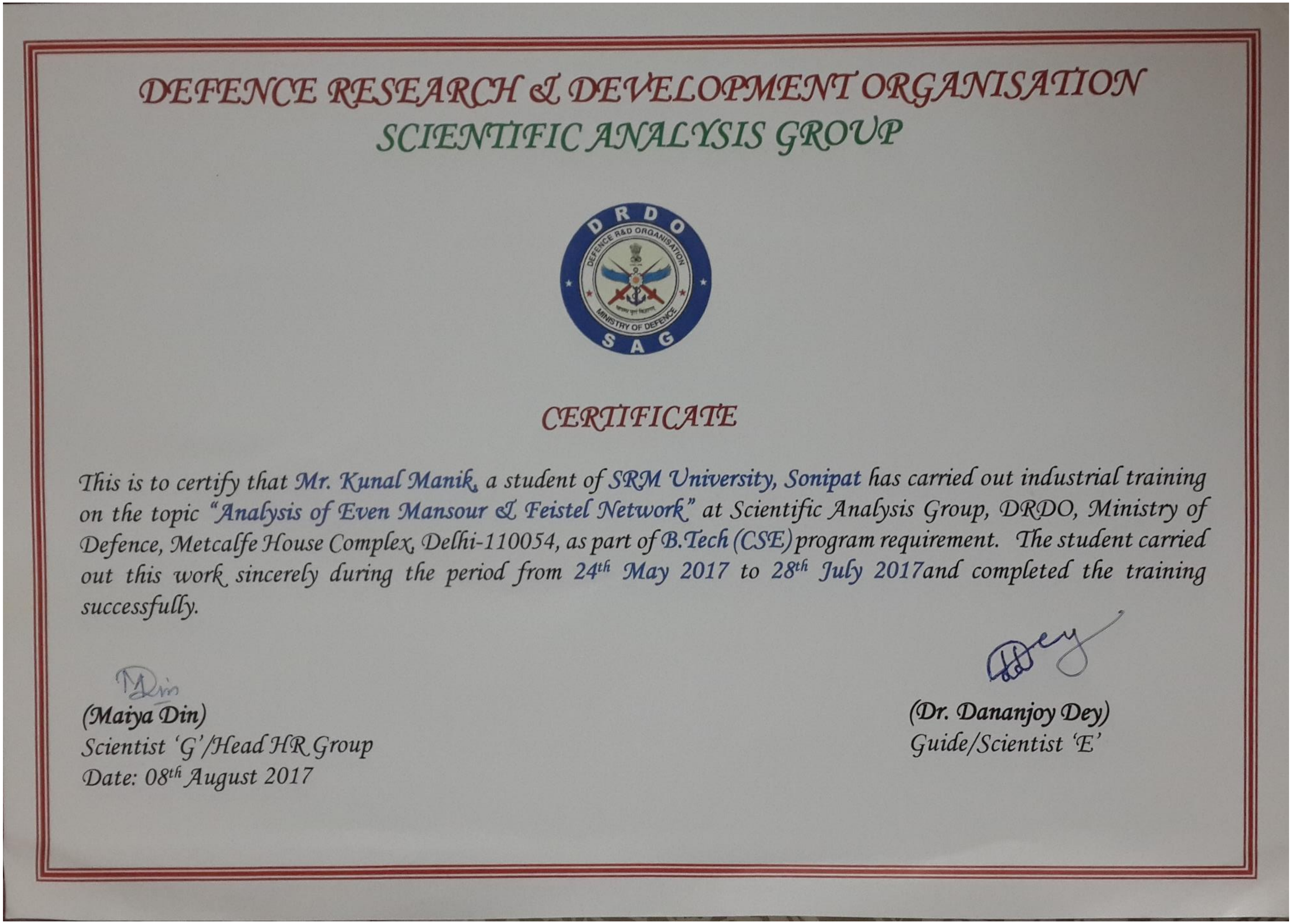
It is to be Certified that the bonafied record submitted by ________________________________, having registration number __________________ of 7th Semester (4th Year) for Bachelor of Technology in Computer Science and Engineering Degree in the Department of Computer Science and Engineering, SRM University has been done for the course INDUSTRIAL TRAINING – II (CS0316) during the academic year 2017 – 2018.

HEAD OF THE DEPARTMENT **FACULTY**

Submitted for the Industrial Training Assessment/Examination held on __________ 2017.

Internal Examiner **External Examiner**

DRDO – SAG LAB, METCALFE HOUSE **SRM UNIVERSITY, DELHI-NCR, SONEPAT**



DEFENCE RESEARCH & DEVELOPMENT ORGANISATION

SCIENTIFIC ANALYSIS GROUP

CERTIFICATE

This is to certify that Mr. Kunal Manik, a student of SRM University, Sonipat has carried out industrial training on the topic "Analysis of Even Mansour & Feistel Network" at Scientific Analysis Group, DRDO, Ministry of Defence, Metcalfe House Complex, Delhi-110054, as part of B.Tech (CSE) program requirement. The student carried out this work sincerely during the period from 24th May 2017 to 28th July 2017and completed the training successfully.

MDin

(Maiya Din)
Scientist 'G'/Head HR Group
Date: 08th August 2017

Dey

(Dr. Dananjoy Dey)
Guide/Scientist 'E'

ACKNOWLEDGEMENT

The research training opportunity I had at DRDO **– SAG Lab, Metcalfe House** was a great chance for learning and professional development. Therefore, I consider myself as a very lucky individual as I was provided with an opportunity to be a part of it. I am also grateful to have a chance to meet so many wonderful people and professionals who led me though this internship period.

Bearing in mind previous I am using this opportunity to express my deepest gratitude and special thanks to the director of DRDO – SAG Lab who in spite of being extraordinarily busy with his duties, took time out to hear, guide and keep me on the correct path and allowing me to carry out my project at their esteemed organization and extending during the training.

I express my deepest thanks to **Dr Dhananjoy Dey**, Scientist, SAG Lab, for taking part in useful decision & giving necessary advices and guidance and arranged all facilities to make the research easier. I choose this moment to acknowledge his contribution gratefully.

I would also like to extend my heartfelt gratitude towards **Dr Ajay Sharma**, Head of Department (Computer Science & Engineering) for constantly supporting me throughout this journey.

I perceive as this opportunity as a big milestone in my career development. I will strive to use gained skills and knowledge in the best possible way, and I will continue to work on their improvement, in order to attain desired career objectives.

Hope to continue cooperation with all of you in the future.

TABLE OF CONTENTS

AIM & OBJECTIVE OF TRAINING

1. Design Analysis of Modern Block Ciphers.
2. Understanding concept of Complex Networks
3. Understanding the importance of Rounds
4. Study of nature of attacks on Modern Block Ciphers
5. Security analysis of Even-Mansour and Feistel Networks

ABOUT THE INSTITUTE

DRDO
SAG Lab, Metcalfe House
(DEPARTMEMT OF DEFENSE MINISTRY, INDIA)

BRIEF PROFILE OF THE COMPANY:

Scientific Analysis Group (SAG) was established in 1963 for evolving new scientific methods for design and analysis of communication systems. It was situated in Central Secretariat Complex and consisted of 12 scientists. This group was placed under direct control of Chief Controller (R&D) in 1973 and became a full-fledged Directorate in R&D Headquarters.

In 1976, SAG started undertaking R&D projects on mathematical, communication and speech analysis. Due to the increasing responsibilities of SAG, the manpower component of SAG underwent expansion and additional accommodation was allotted to SAG at Metcalfe House Complex. SAG was further entrusted with R&D work in the field of electronics. Work related to evaluating communication equipment to be introduced in Services was taken up during 1980. The manpower structure was again revised and the electronic facilities were enhanced. Presently SAG is housed in two independent buildings with a total manpower of 140 scientists/technical and other staff.

Specialties:

- Advanced Mathematical and Statistical Analysis & Development of Tools
- Linguistics - Computational and Structural
- Speech Analysis - Recognition and Synthesis
- Simulation Studies
- Microprocessor-based Systems
- Signal Processing
- Satellite Communication
- High Performance Computing

Address: Scientific Analysis Group, Metcalfe House, Delhi - 110 054

INTRODUCTION TO THE RESEARCH/PROJECT DONE

Cryptography

Cryptography is a science which deals with how to achieve Privacy, Authentication, Integrity and Non-Repudiation. It is an art of writing and solving codes.

Cryptanalysis

Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems.

Block Cipher

Block ciphers operate on “blocks” of data. Such blocks are typically 64 or 128 bits in length and they are transformed into blocks of the same size under the action of a secret key. When using the basic block cipher with the same key, two instances of the same input block will give the same output blocks.

Pseudorandom Function

Pseudorandom functions are efficient and deterministic functions which return pseudorandom output indistinguishable from random sequences. A pseudorandom function, which output is indistinguishable from random sequences, is called a secure one.

Pseudorandom Permutation

A keyed permutation P on a group G is a Pseudorandom Permutation (PRP) over G if it is indistinguishable from a random permutation for all probabilistic distinguishers having access to only polynomially many permutation-oracle queries.

Super Pseudorandom Permutation

A Super Pseudorandom Permutation (sPRP) is permutation where the distinguisher is given access to the inverse permutation-oracle as well.

Indistinguishability and Indifferentiability

Two systems, say **S** and **T,** are said to be *Indistinguishable* if no efficient Algorithm, **D**(.), connected to either **S** or **T** is able to decide whether it is interacting with **S** or **T .**

For the same two systems, they both are *indifferentiable* if given the Oracle '**O**' access, both **S** and **T** are indistinguishable i.e. given the oracle access both **S** and **T** cannot be differentiated. "*Indistinguishablility refers to semantic secrecy.*"

Slide Attack

The **slide attack** is a form of cryptanalysis designed to deal with the prevailing idea that even weak ciphers can become very strong by increasing the number of rounds, which can ward off a differential attack. The slide attack works in such a way as to make the number of rounds in a cipher irrelevant. Rather than looking at the data-randomizing aspects of the block cipher, the slide attack works by analyzing the key schedule and exploiting weaknesses in it to break the cipher. The most common one is the keys repeating in a cyclic manner.

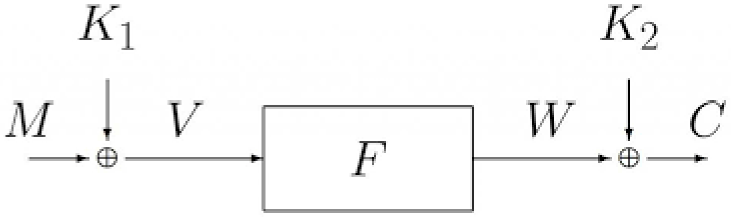
The only requirements for a slide attack to work on a cipher is that it can be broken down into multiple rounds of an identical *F* function. This probably means that it has a cyclic key schedule. The *F* function must be vulnerable to a known-plaintext attack. The slide attack is closely related to the related-key attack.

Even-Mansour Scheme

The encryption (or cryptogram) E_K (M) of a message M ∈ {0, 1} ^{n} by the key K = <K_1, K_2>, is performed by $\mathbf{E_K (M) = F (M \oplus K_1) \oplus K_2}$**;**

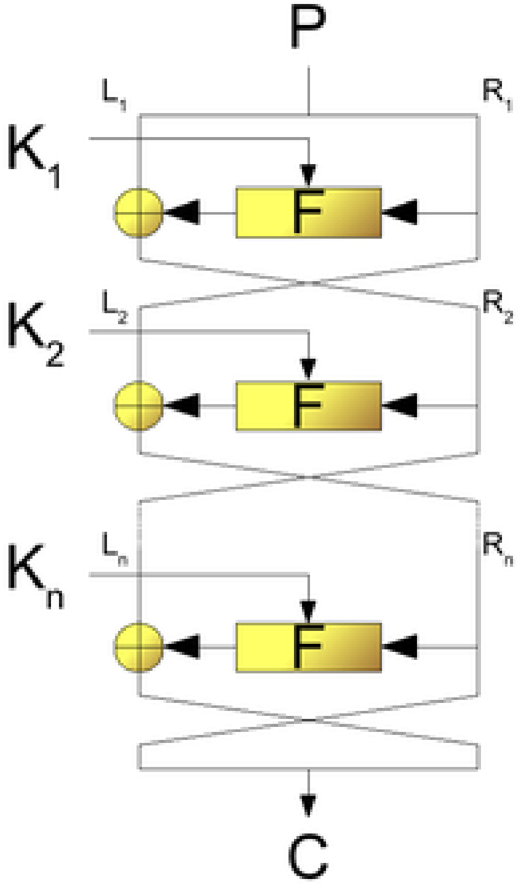
Where ⊕ denotes the bit-by-bit exclusive-or operation.

The decryption of a cryptogram C ∈ {0, 1} ^{n}, is performed by $\mathbf{D_K (C) = F^{-1} (C \oplus K_2) \oplus K_1}$**;**



Feistel Network/Feistel Cipher

A Feistel cipher is a symmetric structure used in the construction of block ciphers, named after the German-born physicist and cryptographer Horst Feistel who did pioneering research while working for IBM (USA); it is also commonly known as a Feistel network. A large proportion of block ciphers use the scheme, including the Data Encryption Standard (DES). The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule. Therefore, the size of the code or circuitry required to implement such a cipher is nearly halved. A Feistel network is an iterated cipher with an internal function called a round function.



INDUSTRIAL TRAINING AND ACADEMIC COURSE RELATION

Related Academic Course: Network Security (CS0427)

TOPIC RELATED TO THE COURSE

Block Ciphers : In cryptography, a block cipher is a deterministic algorithm operating on fixed-length groups of bits, called a *block*, with an unvarying transformation that is specified by a symmetric key. Block ciphers operate as important elementary components in the design of many cryptographic protocols, and are widely used to implement encryption of bulk data.

The modern design of block ciphers is based on the concept of an iterated product cipher. In his seminal 1949 publication, *Communication Theory of Secrecy Systems*, Claude Shannon analysed product ciphers and suggested them as a means of effectively improving security by combining simple operations such as substitutions and permutations. Iterated product ciphers carry out encryption in multiple rounds, each of which uses a different sub key derived from the original key. One widespread implementation of such ciphers, named a Feistel network after Horst Feistel, is notably implemented in the DES cipher. Many other realizations of block ciphers, such as the AES, are classified as substitution-permutation networks.

The publication of the DES cipher by the United States National Bureau of Standards (subsequently the U.S. National Institute of Standards and Technology, NIST) in 1977 was fundamental in the public understanding of modern block cipher design. It also influenced the academic development of cryptanalytic attacks. Both differential and linear cryptanalysis arose out of studies on the DES design. As of 2016 there is a palette of attack techniques against which a block cipher must be secure, in addition to being robust against brute force attacks.

Even a secure block cipher is suitable only for the encryption of a single block under a fixed key. A multitude of modes of operation have been designed to allow their repeated use in a secure way, commonly to achieve the security goals of confidentiality and authenticity. However, block ciphers may also feature as building-blocks in other cryptographic protocols, such as universal hash functions and pseudo-random number generators.

Security (Ciphertext Indistinguishability): Ciphertext indistinguishability is a property of many encryption schemes. Intuitively, if a cryptosystem possesses the property of indistinguishability, then an adversary will be unable to distinguish pairs of ciphertexts based on the message they encrypt. The property of indistinguishability under chosen plaintext attack is considered a basic requirement for most provably secure public key cryptosystems, though some schemes also provide indistinguishability under chosen ciphertext attack and adaptive chosen ciphertext attack. Indistinguishability under chosen plaintext attack is equivalent to the property of semantic security, and many cryptographic proofs use these definitions interchangeably.

A cryptosystem is considered *secure in terms of indistinguishability* if no adversary, given an encryption of a message randomly chosen from a two-element message space determined by the adversary, can identify the message choice with probability significantly better than that of random guessing (½). If any adversary can succeed in distinguishing the chosen ciphertext with a probability significantly greater than ½, then this adversary is considered to have an "advantage" in distinguishing the ciphertext, and the scheme is *not* considered secure in terms of indistinguishability. This definition encompasses the notion that in a secure scheme, the adversary should learn no information from seeing a ciphertext. Therefore, the adversary should be able to do no better than if it guessed randomly.

Security in terms of indistinguishability has many definitions, depending on assumptions made about the capabilities of the attacker. It is normally presented as a game, where the cryptosystem is considered secure if no adversary can win the game with significantly greater probability than an adversary who must guess randomly. The most common definitions used in cryptography are indistinguishability under chosen plaintext attack (abbreviated IND-CPA), indistinguishability under (non-adaptive) chosen ciphertext attack (IND-CCA1), and indistinguishability under adaptive chosen ciphertext attack (IND-CCA2). Security under either of the latter definition implies security under the previous ones: a scheme which is IND-CCA1 secure is also IND-CPA secure, and a scheme which is IND-CCA2 secure is both IND-CCA1 and IND-CPA secure. Thus, IND-CCA2 is the strongest of the three definitions of security.

Task Period	**Week 1 – Week 3**
Resources	**A construction of a Cipher From a Single Pseudorandom Permutation**(Research Paper) **Block Cipher – A Companion**(Book)
Objectives	Identify and analyze the effect of Random permutation(s) on a Cipher Role of Groups & Basic Number Theory
Knowledge Gained	Randomness and Pseudorandomness
Challenges	Generation of Truly Random permutations or Pseudorandom permutations

Task Period	**Week 4 – Week 6**
Resources	**Five Rounds are Sufficient and Necessary for the Indifferentiability of Iterated Even-Mansour**(Research Paper) **Block Cipher – A Companion**(Book)
Objectives	Verifying the Indifferentiability of Even-Mansour Scheme
Knowledge Gained	Distinguishability and Indifferentiability of a Pseudorandom Cipher
Challenges	Indistinguishability and Indifferentiability

Date (Weeks)	**Week 7**
Resources	**Security of Even-Mansour Ciphers under Key-Dependent Messages**(Research Paper)
Objectives	Effect of Keys on Even Mansour
Knowledge Gained	Key dependence in Even Mansour Scheme
Challenges	Key Dependence of an algorithm

Task Period	Week 8 – Week 9
Resources	**How to generate Pseudorandom Permutations Over Other Groups : Even-Mansour and Feistel Revisited**(Research Paper)
Objectives	Analyze the effects of rounds over a group Number of rounds for an algorithm to be super-pseudorandom
Knowledge Gained	Importance of Rounds in a Cipher or Cryptographic Scheme
Challenges	Super-pseudorandomness identification

SUMMARY

Literature Survey

- **Even S. & Mansour Y. - 02 July 1996**

We suggest a scheme for a block cipher which uses only one randomly chosen permutation, F. The key, consisting of two blocks, K1 and K2 is used in the following way, The message block is XORed with K1before applying F, and the outcome is XORed with K2,to produce the cryptogram block. We show that the resulting cipher is secure (when the permutation is random or pseudorandom).This removes the need to store, or generate a multitude of permutations.

- **Hougaard H. - 6 July 2017**

Generalized the Even-Mansour cipher and the Feistel cipher. Shown that Even and Mansour's original notions of secrecy are obtained on a one-key, group variant of the Even-Mansour cipher. Generalized that the Even-Mansour cipher is pseudorandom, to super pseudorandomness, also in the one-key, group case. After generalizing the Feistel cipher to arbitrary groups, resolved an open problem that the 3-round Feistel cipher over an arbitrary group is not super pseudorandom. Finally, shown that the Even-Mansour cipher can be implemented using the Feistel cipher as the public permutation.

- **Dai Y, Seurin Y, Steinberger J & Thiruvengadam A. - 24 Feb, 2017**

We prove that the 5-round iterated Even-Mansour (IEM) construction with a non-idealized key-schedule (such as the trivial keyschedule, where all round keys are equal) is indifferentiable from an ideal cipher. In a separate result, we also prove that five rounds are necessary by describing an attack against the corresponding 4-round construction. This closes the gap regarding the exact number of rounds for which the IEM construction with a non-idealized key-schedule is indifferentiable from an ideal cipher, which was previously only known to lie between four and twelve. Moreover, the security bound we achieve is comparable to (in fact, slightly better than) the previously established 12-round bound.

- **Farshim P, Khati L & Vergnaud D. - 2017**

Formalized that the ideal cipher is KDM secure. Then, showed EM ciphers meet varying levels of KDM security depending on the number of rounds and permutations used. One-round EM achieves some form of KDM security, but this excludes security against offsets of keys. With two rounds we obtain KDM security against offsets, and using different round permutations we achieve KDM security against all permutation-independent claw-free functions.

Research Training Benefits

- Practical use of Cryptography
- Protocol Security
- Importance of Rounds in Security
- Importance of Complex, non-linear structures or schemes
- Writing and Analyzing Research Papers
- Further Advancements in Security
- Industrial needs of Security
- Scope of Research in this field
- Working of Security process of Networks

CONCLUSION

A 1-round EM Scheme is both Indistinguishable and Indifferentiable i.e. both Pseudorandom and super Pseudorandom thereby making this scheme almost unbeatable.

While, a Group Feistel Cipher achieves pseudorandomness only at third round it is not super pseudorandom at this stage albeit a four-round Group Feistel can satisfy super pseudorandomness.

FUTURE SCOPE OF PROJECT

Cryptography in general is the need and greed of everything or scheme that uses or involves Information exchange that happens to be under a closed environment. Based on prominent future aspects, the research based training done here can lead to following fields within Cryptographic Security

1. Block Chain
2. Internet Protocols
3. Advanced Research in XOR Schemes
4. Advanced Research in Methodology of Cryptanalysis

REFERENCES

- Joan Daemen and Vincent Rijmen, The Design of Rijndael AES - The Advanced Encryption Standard, Springer, 2002
- Yuanxi Dai, Yannick Seurin, John Steinberger, and Aishwarya Thiruvengadam, “Five Rounds are Sufficient and Necessary for the Indifferentiability of Iterated Even-Mansour”, February 24, 2017
- E.K. Grossman and B. Tuckerman (1977). "Analysis of a Feistel-like cipher weakened by having no rotating key". IBM Thomas J.Watson Research Report RC 6375.
- Shimon Even and Yishay Mansour. “A construction of a cipher from a single pseudorandom permutation”. Cryptology, 1997.
- Hector Bjoljahn Hougaard, “How to Generate Pseudorandom Permutations Over Other Groups: Even Mansour and Feistel Revisited”, 6 July 2017
- Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography. CRC Press, 2 edition, 2015.
- Lars R. Knudsen and Matthew Robshaw, The Block Cipher Companion, 2011th Edition

WEEKLY PROGRESS REPORTS / END OF THE WEEK REPORTS

Date: 26th May, 2017

Subject: EOD Report

Tasks Completed:

- Basic Concepts and Historical View
- Types of Cryptographic Schemes
- Famous Cryptographic schemes

Thanks

Date: 29th May, 2017

Subject: EOD Report

Tasks Completed:

- Functioning of Enigma
- Mathematical Foundations of Cryptography
- Elements of Number Theory

Thanks

Date: 1st June, 2017

Subject: EOD Report

Tasks Completed:

- Primality Tests
- Computationally hard problems in Number Theory

Thanks

Date: 5th June, 2017

Subject: EOD Report

Tasks Completed:

- Symmetric Key Cryptography
- Feistel Network
- DES

Thanks

Date: 7th June, 2017

Subject: EOD Report

Tasks Completed:

- DES (in detail)
- Concept of S-Box and P-Box
- RC Algorithms

Thanks

Date: 7th June, 2017

Subject: EOD Report

Tasks Completed:

I. Design of Rijndael
II. AES Algorithm
III. Structure and variants of AES

Thanks

Date: 9th June, 2017

Subject: EOD Report

Tasks Completed:

IV. RSA Algorithm

V. Approach and implementation of RSA Algorithm

Thanks

Date: 12th June, 2017

Subject: EOD Report

Tasks Completed:

VI. Randomness

VII. Psuedorandomness

VIII. Brief History of Pseudorandom Algorithms

IX. Super pseudorandom Algorithms

Thanks

Date: 15th June, 2017

Subject: EOD Report

Tasks Completed:

X. Pseudorandom permutation

XI. *A construction of a Cipher from a Single Pseudorandom Permutation*

Thanks

Date: 19th June, 2017

Subject: EOD Report

Tasks Completed:

XII. Distinguishability

XIII. Indifferentiability

Thanks

Date: 23rd June, 2017

Subject: EOD Report

Tasks Completed:

XIV. Distinguishablity in Even Mansour Scheme

XV. Cryptanalysis in symmetric keys

XVI. Attacks on DES

XVII. Attacks on AES

XVIII. Attacks on RSA

Thanks

Date: 25th June, 2017

Subject: EOD Report

Tasks Completed:

XIX. *Five Rounds are Sufficient and Necessary for the Indifferentiability of Iterated Even-Mansour* (Up to Section 3)

Thanks

Date: 30th June, 2017

Subject: EOD Report

Tasks Completed:

XX. *Five Rounds are Sufficient and Necessary for the Indifferentiability of Iterated Even-Mansour* (Up to Section 4)

Thanks

Date: 2nd July, 2017

Subject: EOD Report

Tasks Completed:

XXI. *Five Rounds are Sufficient and Necessary for the Indifferentiability of Iterated Even-Mansour* (Up to Section 5.2)

Thanks

Date: 6th July, 2017

Subject: EOD Report

Tasks Completed:

XXII. *Five Rounds are Sufficient and Necessary for the Indifferentiability of Iterated Even-Mansour* (Up to Section 5.6)

Thanks

Date: 8th July, 2017

Subject: EOD Report

Tasks Completed:

XXIII. *Five Rounds are Sufficient and Necessary for the Indifferentiability of Iterated Even-Mansour*

Thanks

Date: 14th July, 2017

Subject: EOD Report

Tasks Completed:

XXIV. Key Dependence of an Algorithm

XXV. *Security of Even-Mansour Ciphers under Key-Dependent Messages*

Thanks

Date: 18th July, 2017

Subject: EOD Report

Tasks Completed:

XXVI. *How to generate Pseudorandom Permutations Over Other Groups : Even Mansour and Feistel Revisited* (Up to Section 4)

Thanks

Date: 22nd July, 2017

Subject: EOD Report

Tasks Completed:

XXVII. *How to generate Pseudorandom Permutations Over Other Groups : Even Mansour and Feistel Revisited*

Thanks

Date: 24th July, 2017

Subject: EOD Report

Tasks Completed:

XXVIII. Compilation of Results

XXIX. Preparation of Appendix

Thanks

Date: 28th July, 2017

Subject: EOD Report

Tasks Completed:

XXX. Completion of Appendix (Report Submitted to the Mentor)

Thanks

APPENDIX

Chapters

Security and Analysis of Even-Mansour and Feistel Network

1. Introduction

1.1 Cryptology

a. Cryptography

Cryptography is a science which deals with how to achieve Privacy, Authentication, Integrity and Non-Repudiation. It is an art of writing and solving codes.

"Cryptography is about communication in the presence of an adversary."

Modern Cryptography is the scientific study of techniques for securing digital information, transaction and distributed computation. It deals with message authentication, digital signatures, protocols for exchanging secret key, authentication protocols, electronic auctions and elections, digital cash and more.

b. Cryptanalysis

Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems.

1.2 Block Cipher

Block ciphers operate on "blocks" of data. Such blocks are typically 64 or 128 bits in length and they are transformed into blocks of the same size under the action of a secret key. When using the basic block cipher with the same key, two instances of the same input block will give the same output blocks. [1]

The block cipher encrypts a block of plaintext or message m into a block of ciphertext c under the action of a secret key k. This will typically be denoted as c = $\text{ENC}_k(m)$. The exact form of the encryption transformation will be determined by the choice of the block cipher and the value of the key k. The process of encryption is reversed by decryption, which will use the same user-supplied key. This will be denoted m = $\text{DEC}_k(c)$.

In terms of randomness, a block cipher can also be identified as a pseudorandom permutation family operating on fixed-size blocks of bits.

1.3 Randomness

a. Pseudorandom Function

Pseudorandom functions are efficient and deterministic functions which return pseudorandom output indistinguishable from random sequences. A pseudorandom function, which output is indistinguishable from random sequences, is called a secure one.

b. Pseudorandom Permutation

A keyed permutation P on a group G is a Pseudorandom Permutation (PRP) over G if it is indistinguishable from a random permutation for all probabilistic distinguishers having access to only polynomially many permutation-oracle queries.

c. Super Pseudorandom Permutation

A Super Pseudorandom Permutation (sPRP) is permutation where the distinguisher is given access to the inverse permutation-oracle as well.

1.4 Indistinguishability and Indifferentiability

Two systems, say **S** and **T,** are said to be *Indistinguishable* if no efficient Algorithm, **D**(.), connected to either **S** or **T** is able to decide whether it is interacting with **S** or **T .**

For the same two systems, they both are *indifferentiable* if given the Oracle '**O'** access, both **S** and **T** are indistinguishable i.e. given the oracle access both **S** and **T** can't be differentiated. *"Indistinguishablility refers to semantic secrecy."*

1.5 Slide Attack

The **slide attack** [2] is a form of cryptanalysis designed to deal with the prevailing idea that even weak ciphers can become very strong by increasing the number of rounds, which can ward off a differential attack. The slide attack works in such a way as to make the number of rounds in a cipher irrelevant. Rather than looking at the data-randomizing aspects of the block cipher, the slide attack works by analyzing the key schedule and exploiting weaknesses in it to break the cipher. The most common one is the keys repeating in a cyclic manner.

The only requirements for a slide attack to work on a cipher is that it can be broken down into multiple rounds of an identical *F* function. This probably means that it has a cyclic key schedule. The *F* function must be vulnerable to a known-plaintext attack. The slide attack is closely related to the related-key attack.

2. Security of Even-Mansour and Feistel Network

In this report we have generalized the security analysis of Even-Masour Scheme and Feistel Network on the basis of Pseudo-Randomness whether the scheme over a group is pseudorandom or not and given the oracle access can the scheme be identified as super pseudorandom.

Using a "**Slide Attack**" [3] we determine the above bound.

Our main focus in this report will be to determine the security of Even-Mansour cipher and Feistel Network cipher based on the properties of being Indistinguishable and Indifferentiable i.e. whether the cipher can be distinguished from a purely random permutation or not.

Before going to discuss the security, we will define a few terms. [4]

Definition 1 : An algebraic structure <G, •> is called a **group** if the following conditions are satisfied:

1. The operation • is associative, i.e.,

$$\forall_{a,b,c\in G}\ [a \bullet (b \bullet c) = (a \bullet b) \bullet c]$$

2. There exists an identity element e ∈ G which is neutral with respect to the operation •, i.e.

$$\exists_{e\in G}\ \forall_{a\in G}\ [a \bullet e = e \bullet a = a]$$

3. For every element a ∈ G there exists an element ã ∈ G satisfying the following property :

$$\forall_{a\in G}\ \exists_{\tilde{a}\in G}\ [\mathbf{a \bullet \tilde{a} = \tilde{a} \bullet a = e}]$$

If the operation in a group has the symbol +, then it is called addition and the group is called additive. In this case the element ã is denoted by −a and called the inverse element of a. The identity element of an additive group is called the zero of the group and is denoted by 0. In a multiplicative group the operation is called multiplication and is denoted by a dot ·, which is often neglected in the notation, analogously as in the case of multiplying numbers. In this case the inverse element of a is denoted by a^{-1} . The identity element in a multiplicative group has the symbol 1 and is called the unit of the group.

Definition 2 : If the group operation is commutative, i.e.,

$$\forall_{a,b\in G}\ [\mathbf{a \bullet b = b \bullet a}],$$

then the group is called commutative or **Abelian**.

Definition 3 : Let G be a group consisting of a finite number of elements. We call G a **finite group** and the number of its elements the **order of G**. The order of a group G is denoted by **| G |** or **card G**.

Definition 4 : An algebraic structure <R, +, ·> is called a **ring** if the following axioms are satisfied:

1. The structure <R, +> is an Abelian group;

2. The operation · is associative, i.e., $\forall_{a,b,c\in R}\ [(a \cdot b) \cdot c = a \cdot (b \cdot c)]$.

3. The operation · is distributive over +, i.e.,

$$\forall_{a,b,c\in R}\ ([a \cdot (b + c) = a \cdot b + a \cdot c] \wedge [(b + c) \cdot a = b \cdot a + c \cdot a]).$$

Operations + and · are usually called addition and multiplication, however, they are not necessarily these commonly understood number operations.

3. Security Analysis

3.1 Even-Mansour

The encryption (or cryptogram) E_K (M) of a message M $\in \{0, 1\}^n$ by the key K = <K1, K2>, is performed by

$$\mathbf{E_K (M) = F (M \oplus K_1) \oplus K_2;}$$

Where $\oplus$ denotes the bit-by-bit exclusive-or operation. [5]

The decryption of a cryptogram C $\in \{0, 1\}^n$, is performed by

$$\mathbf{D_K (C) = F^{-1}(C \oplus K_2) \oplus K_1;}$$

3.1.1 Two Forms of Security for the Group EM Scheme

3.1.1.1 Existential Forgery Problem

In the existential forgery problem, EFP, the adversary has access to four oracles: **P -oracle, P^{-1} -oracle, E -oracle** and *(unrestricted)* **D-oracle**.

The latter is defined as follows: Presented with any C $\in \{0,1\}^n$, the oracle supplies D_K (C). The task is to find a new pair < M, C >, C = E_K (M); i.e. a pair which does not consist of a query and an answer, as previously supplied by either the E -oracle or the D-oracle.

The Adversary **A** eventually outputs a pair (M, C). If E_k (M) = C, and (M, C) has not been queried before, we say that **A** succeeds.

[6]

3.1.1.2 Cracking Problem or Chosen Plaintext/Ciphertext Problem

The cracking problem, CP, is an attempt (by an adversary, **A**) to decode a given encryption C_0 = E_K (M_0), without any a priori knowledge of the key K . The algorithm, employed by the adversary, has access to the following four oracles : **P -oracle, P^{-1} -oracle, E -oracle** and *(C_0 - restricted)* **D-oracle**.

The latter is defined as follows: Presented with C $\in \{0,1\}^n$ (such that C != C_0) the oracle supplies D_K (C).

The algorithm is successful if it outputs $M_0 = D_K (C_0)$. The success probability of the algorithm is the probability that on a randomly chosen encryption $C_0 = E_K (M_0)$ it outputs M_0 , where all C_0 are equally likely.

For any probabilistic adversary **A**, the success probability of solving the EFP is bounded by :

$$Succ(\mathcal{A}) = Pr_{k,P}\left[EFP(\mathcal{A}) = 1\right] = O\left(\frac{st}{|G|}\right)$$

where s is the number of E/D-queries and t is the number of P/P^{-1} -queries, i.e. the success probability is negligible. **[6]**

3.1.2 Pseudo-Randomness of EM Scheme

For any probabilistic adversary **A**, limited to polynomially many E/D – oracle and P/P^{-1} - oracle queries, the adversarial advantage of A is bounded by

$$Adv(\mathcal{A}) \overset{\text{def}}{=} \left|Pr\left[\mathcal{A}^{P,P^{-1}}_{E_k,D_k} = 1\right] - Pr\left[\mathcal{A}^{P,P^{-1}}_{\pi,\pi^{-1}} = 1\right]\right| = \mathcal{O}\left(\frac{st}{|G|}\right)$$

where s is the number of E/D-queries and t is the number of P/P^{-1} -queries, i.e. the success probability is negligible. Thus, is an sPRP. [*Refer Page 2*]

3.1.3 Slide Attack

Consider the one-key Group Even-Mansour cipher

$E(x) = P (x \cdot k) \cdot k$,

over a group G with binary operation ·, where P is a publicly available permutation oracle. Define the following values:

$x = x,\ y = x \cdot k,\ z = P (y),\ w = E(x) = P (x \cdot k) \cdot k$

We hereby have that **$w \cdot y^{-1} = z \cdot x^{-1}$** . Consider the attack which follows.

1. For **$d = \sqrt{|G|}$** arbitrary values $x_i \in G$, $i = 1. . . d$, and d arbitrary values $y_i \in G$, $i = 1, . . . , d$, query the E-oracle on the x_i's and the P -oracle on the y_i's. Store the values in a hash table as

$(E(x_i) \cdot y_i^{-1} , P (y_i) \cdot x_i^{-1} , i)$,

sorted by the first coordinate.

2. If there exists a match in the above step, i.e. $\mathbf{E(x_i) \cdot y_i^{-1} = P(y_i) \cdot x_i^{-1}}$ for some i, check the guess that $\mathbf{k = x_i^{-1} \cdot y_i}$

For a random pair (x, y) ∈ G^2 it holds that $\mathbf{E(x) = P(y) \cdot x^{-1} \cdot y}$ with probability $|G|^{-1}$, so we only expect a few collisions in the hash table, including the collision by the slid pair where the correct key k is found. The data complexity of the attack is *d E*-oracle queries and *d P*-oracle queries. Hence the bound $d^2 = |G|$, which matches the lower bound given in the proof of "*Pseudo-Randomness of EM Scheme"* [*Refer Page 7*] and *"EFP & CP"* [Refer pages 6, 7].

We have therefore found that our scheme is optimal.

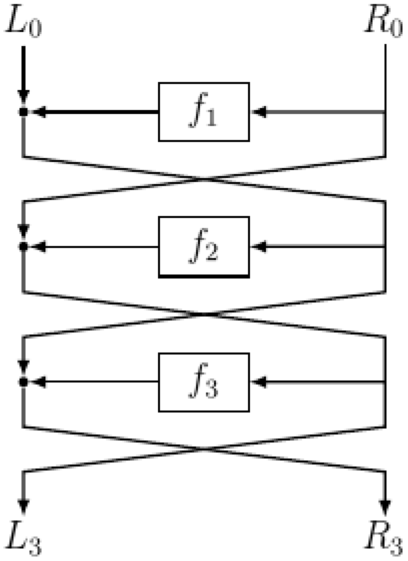
3.2 Feistel Network

Given an efficiently computable but not necessarily invertible function

$\mathbf{f : G \rightarrow G}$, called a *round function,* we define the 1-round Group Feistel cipher $\mathbf{F_f}$ to be

$$\mathbf{F_f : G \times G \rightarrow G \times G,}$$

$$\mathbf{(x, y) \rightarrow (y, x \cdot f(y)).}$$



(a) 3-round Group Feistel cipher.

3.2.1 Pseudo-Randomness of 3 round Group Feistel

If $\boldsymbol{F}$ is a pseudorandom function, then $\boldsymbol{F}^{(3)}$ is a pseudorandom permutation. **[7].** Pseudorandomness of $\boldsymbol{F}$ implies that this has only a negligible effect on the output of any probabilistic polynomial-time distinguisher interacting with $\boldsymbol{F}^{(3)}$ as an oracle.

Let D be a probabilistic polynomial-time distinguisher. Then the following term is negligible.

$$\left|\Pr[D^{\mathsf{Feistel}_{f_1,f_2,f_3}(\cdot)}(1^n) = 1] - \Pr[D^{\pi(\cdot)}(1^n) = 1]\right|$$

$\boldsymbol{F}^{(3)}$ when querying $\boldsymbol{F}$ (with uniform round functions) on a series of q distinct inputs, except with negligible probability the output values $(L^1{}_3 , R^1{}_3), \ldots , (L^q{}_3 , R^q{}_3)$ are distributed such that the $\{L^i{}_3\}$ are uniform and independent, but distinct, n-bit values, and the $\{R^i{}_3\}$ are uniform and independent n-bit values. In contrast, when querying a random permutation on a series of q distinct inputs, the output values $(L^1{}_3 , R^1{}_3), \ldots , (L^q{}_3 , R^q{}_3)$ are uniform and independent, but distinct, 2n-bit values. The best distinguishing attack for D, then, is to guess that it is interacting with a random permutation if Li 3 = Lj 3 for some distinct i, j. But that event occurs with negligible probability even in that case.

Thus, $\boldsymbol{F}^{(3)}$ is not a strong pseudorandom permutation but only a pseudorandom permutation.

Proof : The proof is a counter-example using the following procedure:

1. Choose two oracle pairs in G×G: (L_0, R_0) and (L_0' , R_0) where $L_0 \mathrel{!}= L_0'$.
2. Query the encryption oracle to get (L_3 , R_3) and (L_3', R_3').
3. Query $(L_3'', R_3'') = (L_3', L_0 \cdot (L_0')^{-1} \cdot R_3')$ to the decryption oracle.
4. If $R_0''= L_3' \cdot (L_3)^{-1} \cdot R_0$, guess that P is $\boldsymbol{F}^{(3)}$, else guess random.

For $\boldsymbol{F}^{(3)}$, this algorithm succeeds with probability 1. For a random permutation, this algorithm succeeds negligibly often.

4. Methodology

Points on Obtaining and analysing the result:-

I. **Groups of Research Methods**

Objective knowledge was obtained via means of documented results and theorems in *The Block Cipher Companion* and *Modern Cryptography Primer*. The phenomenon of understanding, however, were resolves via means of careful examination of results and simulated values of the respective research documents.

II. **Content**

The task here is to verify the underlying and open problem of security of Block Ciphers especially Feistel Network and Even-Mansour by simulated and inferential means of methods.

1. Overall methodology requires simulated results, inference knowledge and mathematical proving ability. The base research and analysis is based entirely on these methods.
2. The idea was approached in a symmetrical manner with Convolutions and Theorems running parallel.
3. Following are the equations that are the centre of focus. The equations used in this research are based on the fact which carries the viewpoint of a Distinguisher if it is able to distinguish a Block Cipher from a random permutation or not.

$$Succ(\mathcal{A}) = Pr_{k,P}\left[EFP(\mathcal{A}) = 1\right] = O\left(\frac{st}{|G|}\right)$$

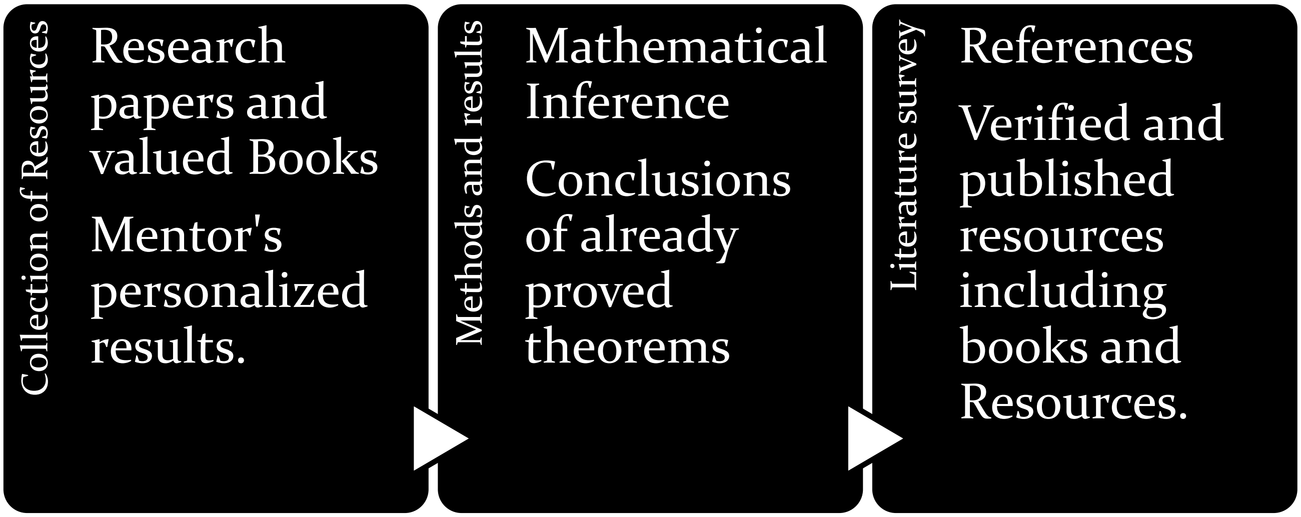
$$Adv(\mathcal{A}) \overset{\text{def}}{=} \left|Pr\left[\mathcal{A}^{P,P^{-1}}_{E_k,D_k} = 1\right] - Pr\left[\mathcal{A}^{P,P^{-1}}_{\pi,\pi^{-1}} = 1\right]\right| = \mathcal{O}\left(\frac{st}{|G|}\right)$$

$$\left|\Pr[D^{\mathsf{Feistel}_{f_1,f_2,f_3}(\cdot)}(1^n) = 1] - \Pr[D^{\pi(\cdot)}(1^n) = 1]\right|$$

4. The results will be proved and analysed using plain probability and inferences used in Number Theory.
5. The limitations include the assumption at the beginning since the proof is based on mathematical tools resembling a simulator while a working machine might differ.

III. Problems to avoid

- Collection and extraction of data was done entirely on the confirmed and appreciated resources including books and research material.
- Every task (except the initial assumption) was kept in mind and the proof was based on the same.
- Literature survey & references are mentioned under **Chapter 5, References** section.
- For the proofs, refer **Chapter 3.** The underlying statements and Theorems have be solved/proved by Mathematical inference and Conclusions proved in other theorems.



Collection of Resources

Research papers and valued Books

Mentor's personalized results.

Methods and results

Mathematical Inference

Conclusions of already proved theorems

Literature survey

References

Verified and published resources including books and Resources.

5. Conclusion

A 1-round EM Scheme is both Indistinguishable and Indifferentiable i.e. both Pseudorandom and super Pseudorandom there by making this scheme almost unbeatable.

While, a Group Feistel Cipher achieves pseudorandomness only at third round it is not super pseudorandom at this stage albeit a four-round Group Feistel can satisfy super pseudorandomness.

6. Future Aspects

Cryptography in general is the need and greed of everything or scheme that uses or involves Information exchange that happens to be under a closed environment. Based on prominent future aspects, the research based training done here can lead to following fields within Cryptographic Security

1. Block Chain
2. Internet Protocols
3. Advanced Research in XOR Schemes
4. Advanced Research in Methodology of Cryptanalysis

References

[1] Lars R. Knudsen and Matthew Robshaw, The Block Cipher Companion, 2011th Edition

[2] E.K. Grossman and B. Tuckerman (1977). "Analysis of a Feistel-like cipher weakened by having no rotating key". IBM Thomas J.Watson Research Report RC 6375.

[3] Hector Bjoljahn Hougaard, “How to Generate Pseudorandom Permutations Over Other Groups : Even Mansour and Feistel Revisited”, 6 July 2017

[4] Joan Daemen and Vincent Rijmen, The Design of Rijndael AES - The Advanced Encryption Standard, Springer, 2002

[5] Shimon Even and Yishay Mansour. “A construction of a cipher from a single pseudorandom permutation”. Cryptology, 1997.

[6] Yuanxi Dai, Yannick Seurin, John Steinberger, and Aishwarya Thiruvengadam, “Five Rounds are Sufficient and Necessary for the Indifferentiability of Iterated Even-Mansour”, February 24, 2017

[7] Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography. CRC Press, 2 edition, 2015.