LIGHT WEIGHT CRYPTOGRAPHY USING PASSIVE RFID TAGS

[1]Mrs.S.Aruna, [2]Rohit.D, [3]V.Seetha Ram Reddy
[1]Asst.Professor, [2,3]B.tech Software Engineering
Software Engineering,
SRM University

***Abstract*—In the recent times RFID has revolutionized field of technology .RFID tags are generally used for tracking purposes. Most existing RFID security protocols utilize more resources which need programming and complex algorithms and also high computational power and thus are unsuitable for RFID tags .In this paper, we present a lightweight secure Communication protocol providing data confidentiality by using traditional cryptography based encryption. Our approach is based on light weight Cryptography using One-time Pad with followed by XOR Encryption on Passive RFID tags**

***Index Terms*— One-time pad, Exclusive-OR, Network Security**

I. INTRODUCTION

Radio Frequency Identification (RFID) tags are electronic components which communicate with other components using the radio signals .They have many applications across various streams around the world [1]. There are two types of RFID tags active and passive. Passive RFID tags need an external scanner or any other component to energize their circuit and communicate [2]. RFID tags can be used as key carriers and can act as excellent communication channels. Due to their low cost and portability they are widely used in fields of cryptography [3].RFID Tags usage will increase in near future [4].This Technology can be widely deployed for Spying and Military purposes [5].

In this Paper we use a One-time pad Encryption followed by an Exclusive-OR (XOR) bitwise Encryption to encrypt the data given by the user and store the data inside the RFID. One Time pad (OTP)is an encryption which cannot be cracked if used correctly since the key is random and used only during encryption and decryption. XOR encryption is also called as modulus 2 addition applying the bitwise XOR operator to every character.

The paper has been structured as follows:
An introduction to Cryptography and a detailed description of the algorithm is provided in section 2 .Section 3 Details the security level of the encryption. The final section provides the results of the conducted research.

II. PROPOSED METHOD

In the paper [2] they have proposed a using XOR One-time pad and modulo addition, they have also posed the problem to store and transfer the key .In the proposed methodology we use a One-time pad modulo addition followed by an XOR bitwise encryption We have also provided a solution to the problem faced in [2] by storing the keys in the RFID and providing several junk values along with it which makes it highly secured.

III. ENCRYPTION/DECRYPTION

Table 1 Encryption/Decryption modules

Symbol	Description
P	Plain text
C	Cipher text
K1	One time pad key
E1	First Encrypted cipher
K2	XOR key
E2	Second Encrypted cipher
HEX	Hexadecimal
S	Security Level of OTP
N	Number of Data Blocks in RFID Tag

Table 2 RFID module

Symbol	Description
T	RFID Tag
B1	Block number of RFID Tag for E2
B2	Block number of RFID Tag for OTP+K1
R	RFID Reader/Writer
A1	User 1
A2	User 2
Q	Intruder

ENCRYPTION

The strength of a good cipher depends on how well the key is hidden. In this proposed method the data is encrypted using OTP and XOR then we store it in the RFID tag.

$(P + K1) \bmod 26 \rightarrow E1$ (1)

The plain text is encrypted using K1 by modulo addition then encrypted as E1 which is the input for next encryption

$E1 \oplus K2 \rightarrow E2$ (2)

The XOR operation is performed on the encrypted cipher E1 and key K2 and the result is second encrypted cipher E2.

T ← R: E2 [B (number)] (3)
T ← R: K1+K2 [B (number)] (4)

The second encrypted key and the keys (K1&K2) are written into RFID tag using the RFID writer into a desired block which the authorized user selects.

READ

Reading the data from the tag shows the junk HEX values. An authorized user (A1, A2) will know which blocks to access , if **Q** tries to access the data he will see only blocks of HEX values and doesn't know the actual data.

T → R: HEX (5)

DECRYPTION

An Authorized user can read the correct Hex values from the Blocks of Tag and can decrypt the Data. The length of OTP is same as that of plane text so an Authorized user can differentiate K1 and K2 from B2 by analyzing the length of E2 from B1.

T → R: HEX (B1, B2) (6)

Authorized user knows which block to access for the data he needs.

HEX (B1) → E2 (7)
HEX (B2) → K1 + K2 (8)

The data from the blocks once decrypted gives E2,K1 and K2.

$E2 \oplus K2 \rightarrow E1$ (9)

The XOR operation is then performed on K2 to give E1.

$(E1 + K1) \bmod 26 \rightarrow P$ (10)
Then the modulo addition operation is performed on E1 and K1 to get the Plain text

IV. SECURITY LEVEL

The security level of the data stored depends upon how well the key is stored. For OTP there are no known ways to decrypt except trial and error or knowing the actual key. In the method which we presented we have further increased the security level(S) of OTP by avoiding its key transfer by paper or network and using an RFID to store it so the security level goes up by **N** times which is **S*N.** Even if the RFID is compromised the intruder gets junk values which was encrypted using XOR , even if this is compromised the resulting text is the OTP cipher once the OTP is changed and the blocks where the plaintext is stored is changed then it gets secured as before.

V. CONCLUSION

In this paper we use a one-time pad encryption followed by an XOR bitwise encryption to encrypt the data and store it safely inside the RFID tag safely by providing many junk values. In this paper we have not only developed a technique for a better usage of one time pad but also solved the problem of storing keys faced in [2].

REFERENCES

[1] Sung jin kim,Young soo kim,Seok cheon park.” RFID security protocol by light weight ECC algorithm”. IEEE,2007.
[2] Dijiang Huang ,Harsh Kapoor. “Towards LightWeight secure Communication Protocols for Passive RFID’s”. IEEE,2009.
[3] Yonghao Gu,Weiming Wu.” Light Weight Mutual Authentication Protocol for ISO 18000-6B Standard RFID”. IEEE,2009.
[4] Jun Feng Fan,Lejla Batina,Ingrid Verbauwhede.” Light Weight implementation options for curve based cryptography: HEEC for RFID”. IEEE,2009.
[5] Mohammad Fal Sadikin,Marcel kyas.” RFID-Tate: Efficient Security and Privacy Protection.