An Efficient Authenticating Short Encrypted Messages Using IND-CPA Algorithms

Amol Akolkar
PG Scholar,
Dept of CSE,
G.H.Raisoni College of Engineering and Management,
Chas village, Ahmednagar, Maharashtra, India.
amolakolkar1990@gmail.com

Vilas Khedekar
Assistant Professor,
Dept of CSE,
G.H.Raisoni College of Engineering and Management,
Chas village, Ahmednagar, Maharashtra, India.
vilaskhedekar2010@gmail.com

Abstract:- In today's age of information and technology , many applications can exchange network of information and communication. In Banking , educational, economical area can also exchange the information over the internet. The exchange of information is too risky to work from internet. So many hackers are try to stolen information from the internet. So there is must require data security and integrity over the internet.There are many authentication Technics are in information technology fields. Like HMAC , UMAC, etc.but all this authentication schemes are time consuming and less secure .so we propose more secure and less time consuming authentication codes that are more useful than any other message authentication code in the our literature survey .

Keywords: *Authentication, IND-CPA Algorithm, Distinguishing attack, chosen plaintext attack, MAC algorithms, Universal Hash-Function Families, Pervasive Computing.*

*****

I. INTRODUCTION

Preserving the integrity of messages exchanged over public channels is one of the classic goals in cryptography and the literature is rich with message authentication code (MAC) algorithms that are designed for the sole purpose of preserving message integrity. Based on their security, MACs can be either unconditionally or computationally secure. Unconditionally secure MACs provide message integrity against forgers with unlimited computational power. On the other hand, computationally secure MACs are only secure when forgers have limited computational power. A popular class of unconditionally secure authentication is based on universal hash-function families, pioneered by Carter and Wegman. Since then, the study of unconditionally secure message authentication based on universal hash functions has been attracting research attention, both from the design and analysis standpoints. The basic concept allowing for unconditional security is that the authentication key can only be used to authenticate a limited number of exchanged messages. Since the management of one-time keys is considered impractical in many applications, computationally secure MACs have become the method of choice for most real-life applications. In computationally secure MACs, keys can be used to authenticate an arbitrary number of messages. That is, after agreeing on a key, legitimate users can exchange an arbitrary number of authenticated messages with the same key. Depending on the main building block used to construct them, computationally secure MACs can be classified into three main categories: block cipher based, cryptographic hash function based, or universal hash-function family based. CBC-MAC is one of the most known block cipher based MACs, specified in the Federal Information Processing StanB. Alomair and R. Poovendran are with the Department of Electrical Engineering, University of Washington, and Seattle, WA, 98195 e-mail: falomair,rp3g@uw.edu. dards publication 113 and the International Organization for Standardization ISO/IEC 9797-1. CMAC, a modified version of CBC-MAC, is presented in the NIST special publication 800-38B, which was based on the OMAC of. Other block cipher based MACs include, but are not limited to, XOR-MAC and PMAC. The security of different MACs has been exhaustively studied. The use of one-way cryptographic hash functions for message authentication was introduced by Tsudik in. A popular example of the use of iterated cryptographic hash functions in the design of message authentication codes is HMAC, which was proposed by Bellare et al. in. HMAC was later adopted as a standard. Another cryptographic hash function based MAC is the MDx-MAC proposed by Preneel and Oorschot. HMAC and two variants of MDxMAC are specified in the International Organization for Standardization ISO/IEC 9797-2. Bosselaers et al. described how cryptographic hash functions can be carefully coded to take advantage of the structure of the Pentium processor to speed up the authentication process. The use of universal hash-function families in the Carter Wegman style is not restricted to the design of unconditionally secure authentication. Computationally secure MACs based on universal hash functions can be constructed with two rounds of computations. In the first round, the message to be authenticated is compressed using a universal hash function. Then, in the second round, the compressed image is

processed with a cryptographic function (typically a pseudorandom function1). Popular examples of computationally secure universal hashing based MACs include, but are not limited to.[1]

II . RELATED WORK

IND-CPA security is a security definition for private- or public-key encryption schemes. At a high level, IND-CPA security means that no adversary can distinguish between encryptions of different messages, even when allowed to make encryptions on its own.

The "IND" part of the name IND-CPA comes from the fact that it is an indistinguishability-based security definition (the adversary tries to distinguish between encryptions of two different messages). The "CPA" part stands for chosen plaintext attack, because in the IND-CPA model, adversaries are allowed to compute encryptions of plaintexts that they can choose.

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 (1⁄2). If any adversary can succeed in distinguishing the chosen ciphertext with a probability significantly greater than 1⁄2, 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.[11][12]

III THE PROPOSED SYSTEM

Let N_1be a bound on the length, in bits, of changed messages. That is, messages to be documented are now not than (N_ 1)-bit long. Select p to be AN N-bit long prime integer. (If N is just too tiny to supply the required security level, p is chosen massive enough to satisfy the specified security level.) Select A number ks uniformly randomly from the multiplicative cluster ZZ_ p; ks is that the secret key of the theme. The prime number, p, and the secret key, ks, area unit distributed to legitimate users and can be used for message authentication. Note that the worth of p needn't be secret, solely American state is secret. Let E be any IND-CPA secure cryptography formula. Let m be a brief messages (N_1 bit or shorter) that's to be transmitted to the supposed receiver in an exceedingly confidential manner (by encrypting it with E). Rather than authenticating the message employing an ancient MAC algorithm, take into account the subsequent procedure. On input a message m, a random nowadays r 2 ZZp is chosen. (We overload m to denote each the binary string representing the message, and the integer illustration of the message as a component of ZZp. a similar applies to ks and r. The distinctions between the two representations are omitted once it's clear from the context.) We assume that integers representing distinct messages are distinct.[12].

IV. NOTATIONS AND PREFACES

.1 Notations

- Used Zp as the usual notation for the finite integer ring with the multiplication and addition modulo p.
- Used Zp* as the usual notation for multiplicative group modulo p.
- For two strings a andb of same length, (a ⊕b) is the bitwise exclusive-or (XOR) operation.
- For any two strings aandb, (a || b) denotes the concatenation operation.

4.2 Negligible functions

A function negl: N->R is said to be negligible if it converges to zero faster than the reciprocal of any polynomial function [2].

4.3 Indistinguishability under Chosen Plain Text Attacks

Indistinguishability under chosen plain text attack (IND-CPA) is the important security notion for encryption. Let A be an adversary who has access to oracle to an encryption algorithm, *E*, and ask the oracle to encrypt a polynomial number of messages to get their equivalent cipher texts. The encryption algorithm is said to be IND-CPA secure, if the adversary after calling the encryption a polynomial number of times is given a cipher text corresponding to one of the two plain text messages cannot determine the plaintext message corresponding to the given cipher text with an advantage higher ½.*E* is said to be IND-CPA secure, if adversary's advantage of determining plaintext corresponding to given cipher text <= ½+Negl (N), where N is security parameter, usually the length of the secret key .

V. METHODOLOGY

In a mobile environment, a number of users act as a network nodes and communicate with one another to acquire location based information and services. In a significant portion of such applications, the confidentiality and integrity of the

ISSN: 2321-8169
4526 - 4529

communicated messages are of particular interest. By taking advantage of the fact that the message to be authenticated must also be encrypted, we propose provably secure authentication codes that are more efficient than any message authentication code in the literature. Following

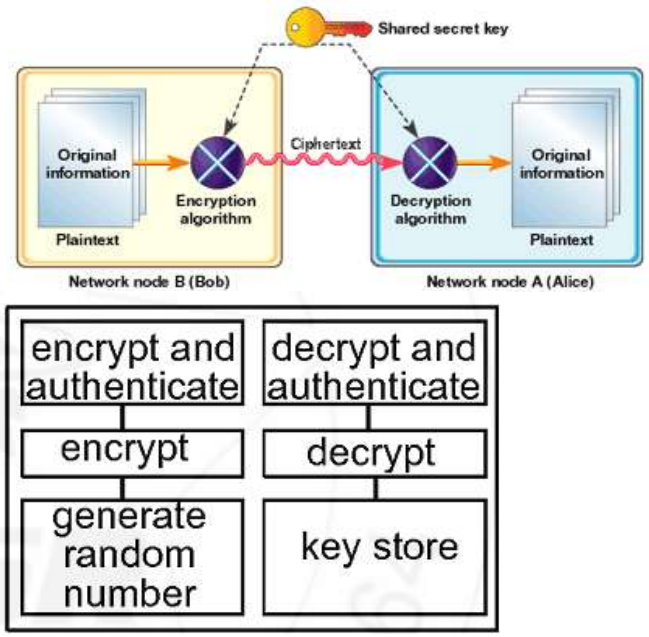


Figure 2: Generalize system.

There will be five modules. 1) Authenticate short messages and encrypt those messages: In this module, first validation plot that might be utilized with any IND-CPA secure encryption calculation. A critical presumption is that messages to be verified are no more than a predefined length. This incorporates applications in which messages are of settled length that is known from the earlier, for example, RFID frameworks in which labels need to validate their identifiers, sensor hubs reporting occasions that have a place with certain area or estimations inside a certain extent[14]

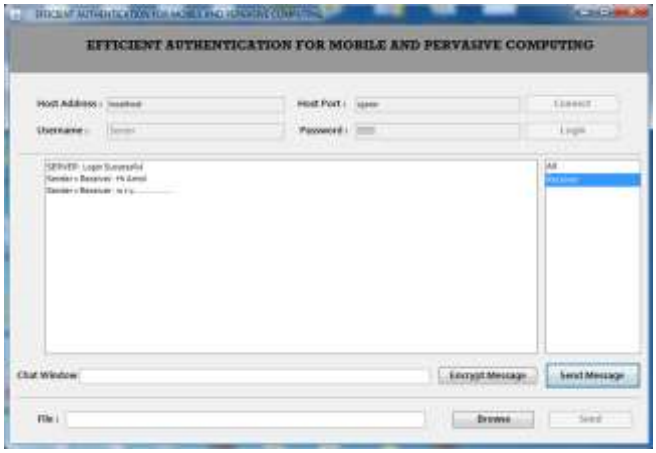
VI EXPERIMENTAL RESULTS

In this project user can send the message from the sender to receiver. Enter the message in the text box and click on **"Encrypt"** button.

Internally IND-CPA Algorithm will take a random number, key and prime number with a message; it will generate a cipher text.

Click on **"Send"** Button. Then it will send the encrypted message to the Receiver

At the Receiver end it will be in decrypted mode, the viewer can't see the process of decryption the user directly will read that message



VII . CONCLUSION

In this project we can studying a new technology for validating small encrypted messages is observe. The key fact is that message which is to be passed over internet must need to be encrypted using IND-CPA Algorithm. Indistinguishability under chosen plain text attack (IND-CPA) is the important security notion for encryption practically it has been proved in this project that if security parameter (the length of the secret key) is less than the advisory advantage value then the given plan text is secure using IND-CPA Algorithms . this algorithm is also useful for short message also. The key value generated for each process is also different for different plaintext. The all experiment in this project prove that IND-CPA algorithm require short time and less energy to encrypt and decrypt the message(Plain text) in network.

VIII. REFERENCES

[1] Efficient Authentication for Mobile and Pervasive Computing Basel Alomair · Radha Poovendran .
[2] Jump up^ iang (2006-05-20). "Indistinguishable from random". Retrieved 2014-08-06.
[3] Jump up^ Bernstein, Daniel J.; Hamburg, Mike; Krasnova, Anna; Lange, Tanja (2013-08-28). "Elligator: Elliptic-curve

ISSN: 2321-8169
4526 - 4529

points indistinguishable from uniform random strings" (PDF). Retrieved2015-01-23.

[4] Jump up^ Möller, Bodo (2004). "A Public-Key Encryption Scheme with Pseudo-random Ciphertexts". doi:10.1007/978-3-540-30108-0_21.

[5] Jump up^ Moore, Cristopher; Mertens, Stephan (2011). The Nature of Computation. ISBN 9780191620805.

[6] Jump up^ Reingold, Omar (November 1998). "Pseudo-Random Synthesizers, Functions and Permutations" (PDF). p. 4. Retrieved 2014-08-07.

[7] Jump up^ Rogaway, Phillip (2004-02-01). "Nonce-Based Symmetric Encryption" (PDF). pp. 5–6. Retrieved 2014-08-07.

[8] E. Gilbert, F. MacWilliams, and N. Sloane, Codes which detect deception, Bell System Technical Journal 53 (1974), pp. 405–424.

[9] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, "SPINS: Security protocols for sensor networks," Wireless networks , vol. 8, no. 5, pp. 521–534, 2002.

[10] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Communications of the ACM , vol. 47, no. 6, pp. 53–57, 2004.

[11] "http://crypto.cs.uiuc.edu/wiki/index.php/IND-CPA_security"

[12] "https://en.wikipedia.org/wiki/Ciphertext_indistinguishability

[13] "http://arxiv.org/ftp/arxiv/papers/1303/1303.0598.pdf

[14] http://ijsetr.com/uploads/152346IJSETR3628-719.pdf