International Journal of Advanced Science and Technology
Vol. 12, November, 2009

Wi Fi Protected Access-Pre-Shared Key Hybrid Algorithm

Maricel O. Balitanas

Hannam University, Department of Multimedia Engineering, 306 791
jhe_c1756@yahoo.com

Abstract

Potentially large number of cryptography solutions to attain security is widely known and recognized. Looking for a stronger scheme is the aim of most researchers to hide valuable information from each other. In this information age, many encryption algorithm exist to help keep information secure and these algorithms vary in complexity and ability to resist cracking. In this paper we present a hybrid crypto scheme that combines the acclaimed effective in symmetric type of algorithm, AES and the Elliptic Curve Cryptography in Asymmetric algorithm.

Keywords: *Hybrid Cryptography, AES, ECC.*

1. Introduction

Looking for a stronger encryption has been on the hunt. People have been searching for ways to hide valuable information from each other. In earlier times man would make a simple pattern changes to an alphabet or substitute other letters or numbers into their written messages, to successfully hide private information.

In this information age many encryption algorithms exist to help keep our information secure. These algorithms vary in complexity and ability to resist cracking. In Ciphers there are two major types, symmetric and asymmetric. Each has their own advantages and disadvantages. Symmetric cipher is significantly faster than asymmetric cipher. Some of the most popular encryption algorithms developed to date are DES, TripleDES, RC2, RS4, Blowfish, Twofish and Rijndael. The mentioned ciphers are symmetric encryption algorithm which means simple use the same key to both encrypt and decrypt data. There are several asymmetric algorithm in existence today, including RSA, DSA, EIGamal and ECC. Currently, the most popular is RSA which means Rivest, Shamir and Adleman, the names of its inventors. [1] ECC is not actually an algorithm but an alternate algebraic system for implementing algorithm, such as DSA using peculiar mathematical objects known as elliptic curve over finite fields.

Wi-Fi Protected Access (WPA and WPA2) is a standard by WiFi Alliance to indicate compliance with the security protocol to secure wireless computer networks. WPA is a recommended solution to WEP security problem it runs on the same hardware that WEP does. The protocol implements the majority of the IEEE 802.11i standards, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. Specifically, the TKIP (temporal Key Integrity Protocol), was brought into WPA. TKIP could be implemented on pre-WPA wireless network interface cards that begun shipping as far back as 1999 through firmware upgrades. As mentioned above there are popular encryption algorithm commonly used. Table 1 depicts the comparison outlining the basics for

the most popular ciphers. [1] Clearly, Rijndael is the most secure cipher out there and for most vendors of WPA implementation use AES (Advance Encryption Standard). The standard comprises three block ciphers, AES -128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. In this paper we are going consider the algorithm of AES in WPA PSK mode cross with the asymmetric algorithm of Elliptic curve cryptography.

The rest of this paper is organized as follows. We first review the most relevant work. Then in Section 3 we present the crossed crypto-scheme algorithm as well as deals with collaborative findings of the study, while Section 4 will present the future works and 5 draws the main conclusions

Table 1. Comparison of the Most Popular Ciphers

Algorithm	Created by	Key size	Algorithm Structure	Existing Crack
Rijndael	Joan Daemon &Vincent Rijmen 1998	128 bits, 192 bits or 256 bits	Substitution permutation Network	Side Chanel attacks
Twofish	Bruce Schneir 1993	128 bits, 192 bits or 256 bits	Feisel Network	Truncated differential cryptanalysis
Blowfish	Bruce Schneier	32-448 bits in steps of the 8 bits 128 bits by default		Second-order differential attack
RC4	Ron Rivest 1987	Variable	Stream	Distinguishers based on weak key schedule
RC2	Ron Rivest 1987	8-128 bits in steps of 8 bits 64 bits by default	Source-Heavy Feistel Network	Related-Key attack

2. Related Studies

One research related to this study is the work done by Shanti M. [2] In these research they have pointed out that The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping and to prevent unauthorized access to a wireless network. WEP relies on a secret key that is shared between a mobile station and an access point. The mode of operation makes stream ciphers vulnerable to several attacks. So improve the security of WEP by using hybrid encryption technique. In this hybrid encryption approach, the information sent from the sender is converted using AES-Rijndael symmetric encryption algorithm with key value. The receiver public key using RSA algorithm encrypts 128-bit key value. Both encoded values are sent to the public network. The receiver receives the encoded information with AES-Rijndael to identify the original information. The AES-Rijndael algorithm is block cipher algorithm. The stream cipher algorithm drawbacks completely removed in this approach. This approach implements secure hash functions. This will avoid the CRC-32 drawbacks like flipping nth bit. Initialization vector (IV) role is completely removed. So, the IV related drawbacks are avoided. Thus this project improves security in wired equivalent privacy algorithm. In our paper we however use the hybrid approach to WPA..

3. The Crossed Crypto-scheme

The most recent physical security protocol, Wi-Fi Protected Access (WPA) and the emerging 802.11i standard, both specify 802.1 x securities as a framework for strong wireless security. 802.1x use authentication, it requires user to provide credentials to security server before getting access to the network. The credentials can be in the form of user name and password, certificate, token or biometric. The security server authenticates the user's credentials to verify that the user is who he or she claims to be and is authorized to access the network. The security server also verifies that the access point is a valid part of the network. This is done to protect the user from connecting to an authorized access point that may have been set ups to fraudulently capture network data.

3.1 Asymmetric Encryption

This method employs a pair of keys, consisting of a public key and a private key. The algorithm used in asymmetric encryption, such as RSA are usually based on solving number-theoretical problems. The security of these algorithms is assured by the inherent difficulty of solving such problem. Example is decomposing large amount into their prime factors. Asymmetric is more acceptable solution for e-commerce, the world is currently promoting encryption as the transaction without the prior requirement to exchange key or secrets. The e-commerce world is currently promoting asymmetric encryption as the solution to all the security need. The advantage of asymmetric is in its functionality. It provides security in a wide range of applications that cannot be solved using only symmetric techniques. [3] [4] However, we pay a price for this in a computational efficiency and increased cost. The following figure shows the typical Asymmetric encryption.

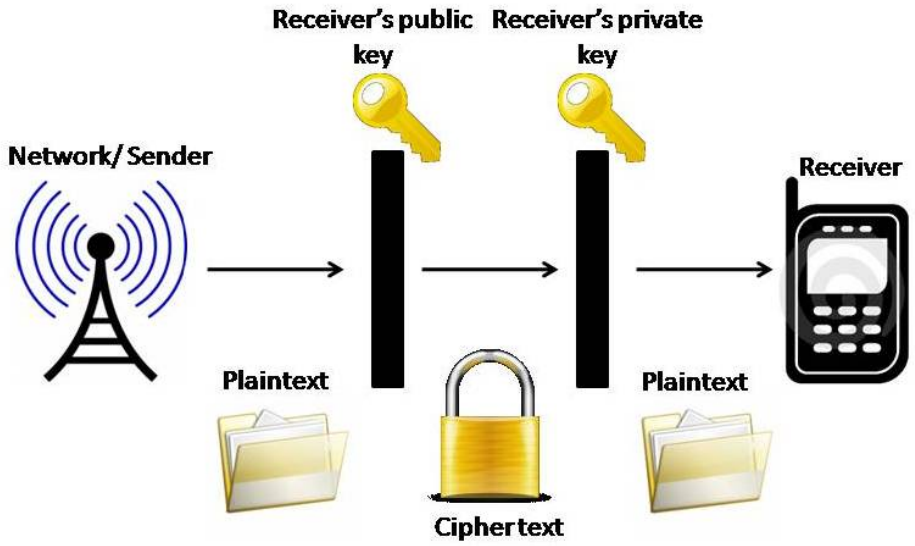

Figure 1. Asymmetric Encryption

1) RSA as asymmetric

RSA (Rivest, Shamir and Adleman) is widely used public key stream. It is an asymmetric key system, which uses variable key sizes. 512-bit, 1024-bit and 2048-bit RSA are the most

common. Its security lies in the difficulty of factoring large composite integers. Although RSA is the most popular Asymmetric cryptography, ECC offers a smaller key sizes, faster computation, as well as memory, energy and bandwidth savings and is thus better suited for small devices.

The difficulty of the encryption process lies in the size of the integers involved in the modular exponentiation. In 512-bit RSA, M, e and n are potentially 512-bit number, which cannot be represented in standard integer's formats

$$C = M^{e} \bmod n \quad (1)$$

2) ECC as asymmetric:

Elliptic Curve Cryptosystem, few years ago, ECC was still a new cryptosystem and researchers did not know if ECC schemes could be implemented efficiently and securely. Since then, researchers have studied ECC and determined it is stronger, more efficient technology that is ideally suited for resource-constrained environments such as smart cards, cell phones, and personal digital assistants (PDSs). [8] Moreover, due to the apparent hardness of the underlying elliptic curve discrete logarithm problem (ECDLP), ECC systems ae also suited for applications that need long-term security requirements. This requires much less processing while at the same time being much harder to crack. For instance, a 256-bit ECC key is a secure as a 3,072-bit RSA key. An elliptic curve E over a field F is defined by the Weierstrass equation: [5]

$$E/F: y^2 + a_1xy + a_3y = x^3 + a2x^2 + a_4x + a_6 \text{ with } a_1, a_2, a_3, a_4, a_6 \in F. \quad (2)$$

An important characteristic of elliptic curves is that the points on the elliptic curves form a group. Details of this elliptic curve you may refer to [6]. Various researchers have proved that ECC requires more time to break as compared to RSA and DSE Certicom [7]], In Certicom the result of their study had been summarized: ECC provides greater efficiency than either integer factorization systems or discrete logarithm systems, in terms of computational overheads, key size and bandwidth. In implementation, these savings mean higher speeds, lower power consumption, and code size reductions. ECC has been accepted as a standard by various bodies.

There are two most common choices for implementation of ECC:

1. Galois Field GF(2m), also known as characteristic two or even (containing 2^m elements, where m is an integer greater than one). In this case, the following equation

$$E/F: y^2 + a_1xy + a_3y = x^3 + a2x^2 + a_4x + a_6 \text{ with } a_1, a_2, a_3, a_4, a_6 \in F.$$

….becomes

$$E/F: y^2+xy=x^3+ax+b \text{ where a and } b \in F, b\neq 0$$

Together with a point at infinity o

2. Galois Field GF(p), also known as integers modulo p. odd, or odd prime (containing p elements, where p is an odd prime number). In this case, equation (2) can be simplified to the form $\mathbf{E/F : y^2 = x^3 + ax + b}$ where **a** and **b** ϵ **F** and $4a^3 + 27b\mathbf{2} \neq 0$ together with a point at infinity (o)

Elliptic curve's important characteristics are that the points on the elliptic curves form a group. Details on ECC can be had from [10] [11][12][13][14][15]
Various researchers have proved that ECC requires more time to break as compared to RSA and DSA. [16] Summarizes the results of their study as" ECC provides greater efficiency than either integer factorization systems or discrete logarithm systems, in terms of computational overheads, key sizes, and bandwidth. In implementation, these savings mean higher speeds, lower power consumption, and code size reductions. ECC has been accepted as a standard by various bodies. Some of them are ANSI (American National Standards Institute). FIPS (Federal Information Proceeding Standards), IEEE P1363 (Institution of Electrical & Electronic Engineers) and WAP (Wireless Application Protocol) .

3) Benefits of ECC over RSA

The significant smaller parameter used in ECC than with RSA is an advantage that can be gained from smaller parameters included in speed and smaller keys or certificates. These advantages are specifically important in environments where at least one of the following resources is limited:

- Power consumption
- Processing power
- Storage space
- Bandwidth

Table 2. Nist Guidelines for Public-Key Sizes with Equivalent Security Levels [8]

Security (Bits)	Symmetric encryption algorithm	Minimum Size (Bits) of Public Keys		
		DSA/DH	RSA	ECC
80	Skipjack	1024	1024	160
112	3DES	2048	2048	224
128	AES-128	3072	3072	256
192	AES-192	7680	7680	384
256	AES-256	15360	15360	512

Thus, ECC is especially well suited for constrained environments such as smart cards, cellular phones, PDAs, digital postage marks, to name a few. 128-bit protection is necessary to achieve relatively lasting security. To avoid compromising the security of the system, NISTs FIPS 140-2 standard indicates that keys for symmetric cipher such as AES must be

matched in strength by public-key algorithm such as RSA and ECC. Depicted in table 2 , while ECC key sizes scale linearly, RSA does not. The gap between systems grows as the key sizes increase. This is relevant to implementations of AES where at 256-bit security one needs RSA key size of 15, 360 bits compared to 512 bits of ECC.[9]

This depicts a significant impact on a communication system as the relative computational performance advantage of ECC versus RSA is not indicated by key size but by the cube of the key sizes. The difference becomes even more intense as the greater increase in RSA key sizes leads to an even greater increase in computational cost. Thus, from 1024-bit RSA key to 3072-bit RSA key requires about 27 times as much computational while ECC would only increase the computation cost by just over 4 times.

To a system that uses 1024-bit RSA, this has important design implications. For instance, ECC-160 has 6X smaller key-size than RSA-1024 and can generate a signature 12 times faster. The performance advantage of ECC stands out even more in higher security levels and at hardware implementations. The following table summarizes it.

Table 3. Hardware Implementation of ECC and RSA [8]

Hardware comparison: 128-bit security level		
mode	RSA-3072	ECC-283
Space-optimized (same clock speed)	(VLSI Cores) 184 ms 50,000 gates	(Grobschadl) 29 ms (16ms for Koblitz curve) 6,660 gates
Speed-optimized (same clock speed)	(VLSI Cores) 110 ms 189,200 gates	(Orlando and Paar) 1.3 ms 80,100 gates

3.2 Symmetric Encryption

Symmetric cryptography involved two parties who share a joint secret or key. This exclusive knowledge of the key enables private and secure communications between the two parties. Without the threat of a third party eavesdropping or otherwise tampering with messages in transit. In this instance, the same key is used for encryption and decryption. Figure 2 depicts a Shared Secret Key mode of a Symmetric Encryption [4]

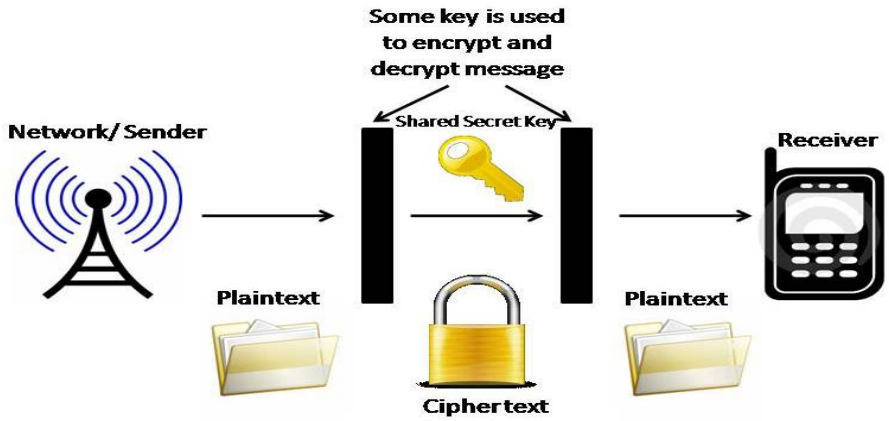

Figure 2. Shared Secret Key mode of a Symmetric Encryption

1) AES in Pre-shared Key mode

Pre-shared key mode is one of the operation modes of WPA it is also known as Personal mode. It is designed for home and small office networks that don't require complexity of 802.11i authentication server. Each wireless network device encrypts the network traffic using a 256 bit key. This key may be entered either as a string of 64 hexadecimal digits, or as a passphrases of 8 to 63 printable ASCII characters. Shared-key WPA is vulnerable to password cracking attacks if a weak passphrase is used. To protect against brute force attack, a 13 character truly random passphrase is sufficient.[2] The structure and algorithm of AES is as follows:

This cipher is an iterative clock cipher. It therefore consists of a sequence of transformation to encipher or decipher the data. The encryption and decryption begin at the end with the step to mix sub keys with the data block. To decipher a block data, one must perform an Add Round key step (XORing a subkeys with the block) by itself, then the regular transformation rounds, and then a final round with the Mix column step omitted.. The cipher itself is defined by the following steps:

- An initial Round Key addition
- Nr-1 Rounds
- A final round

N_b: block length (number of words)
N_k: key length (number of words)
N_r: number of rounds, depending on N_b, N_k
State: a vaiable of N_b words, holding the data block, viewed as a 4 x N_b matric of bytes
Each colum is a word (4 bytes)

Key schedule : N_r + round keys key_0, key_1,…,key_N are computed from the main key *k*

Input: plaintext *m*, key *k*
State ← *m*
AddKey(state, key$_0$)
For i ← *1 to N, -1 do*
    SubBytes (state)
    ShiftRows(state)
    Mixcolumns(state)
    AddKey(state,key)
SubBytes(state)
ShiftRows(state)
AddKey(state, key)
Return(state)

3.3 Crossed Crypto-scheme

To provide the confidentiality of message transmitted over the network is a vital issue. The use of cryptographic system is increasing gradually and the hybrid cryptosystem is widely adopted and used. In this paper a new hybrid cryptosystem is presented in the form of crossed cryptosystem capable of providing implicit authentication for the sender's identity. From the two major types of encryptions we can conclude that Asymmetric encryption provides more functionality than symmetric encryption, at the expense of speed and hardware cost. On the other hand symmetric encryption provides cost-effective and efficient methods of securing data without compromising security and should be

considered as the correct and most appropriate security solution for many applications. In some instances, the best possible solution may be the complementary use of both symmetric and asymmetric encryption. Diagram of a crossed crypto-scheme is shown in Figure 3.

The algorithm presented here combines the best features of both the symmetric and asymmetric encryption techniques. The plain text data is to be transmitted in encrypted using the AES algorithm. Further details on AES can be taken from [9].

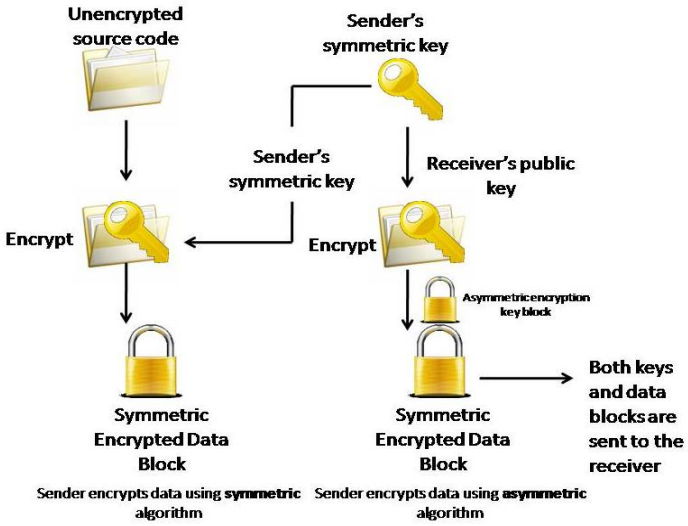

Figure 3. Crossed crypto-scheme

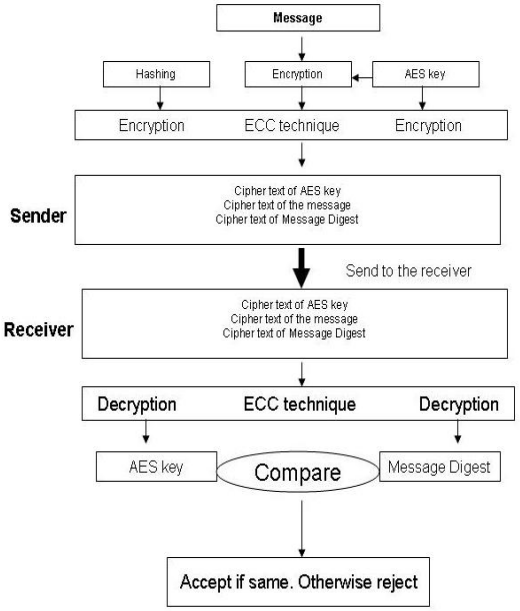

Figure 4. Chain of operation

The AES key which is used to encrypt the data is encrypted using ECC. The cipher text of the message and the cipher text of the key are then sent to the receiver. The message digest by this process would also be encrypted using ECC techniques. The cipher text of the message digest is decrypted using ECC technique to obtain the message digest sent by the sender. This value is compared with the computed message digest. If both of them are equal, the message is accepted otherwise it is rejected. Figure 4 depict this scenario.

Ultimately using ECC, the benefits of ECC are many: Linear scalability, small software footprint. Low hardware implementation costs, low bandwidth requirements, and high device performance. With the use of AES and ESS an essential components of communication today continue to be so for the long term. ECC is a superior algorithm when it comes enabling that security. Since, it offers the highest strength-per-bit of any public key cryptography system today.

4. Future Works

In the future the researchers will implement the crossed crypto-scheme in a messenger set up since such is susceptible to dictionary attacks, which can be deduced through exhaustive searches. The secret keys used in the application will be randomly generated. In the future Further, Implementation of HECC to eliminate the need of large public key size, particularly important in a small devices will be a consideration.

5. Conclusion

Ideally studies are conducted to anticipate potential breaches of security in any system. This algorithm is presented to be implemented in a wireless device application through which recent technologies are more inclined. This experience can be leveraged to refine the assessment implementation process and provide better options of algorithm.

References

[1] https://mentor.ieee.org/802.11/file/08/11-08-1127-12-000m-tgmb-issues-list.xls. "The use of TKIP is deprecated. The TKIP algorithm is unsuitable for the purposes of this standard"
[2] Weakness in Passphrase Choice in WPA Interface, by Robert Moskowitz. Retrieved March 2, 2004
[3] http://www.cs.technion.ac.il/~biham/
[4] http://www.rsasecurity.com/rsalabs/faq/index.html
[5] Cohen H , Gerhard Frey, Handbook of Elliptic and Hyper-elliptic curve Cryptography, Chapman & Hall /CRC, NW, FL, 2006
[6] Blake I, G. Seroussi and N. Smart (eds). Advances in Elliptic Curve Cryptography , Cambridge University Press, 2005
[7] Certicom whitepaper, Remarks on the Security of the Elliptic Curve Cryptosystem.. September 1997.
[8] http://www.design-reuse.com/articles
[9] http://csrc.nist.gov/publications/fips/fips197/fips -197.pdf
[10] Blake I, G. Seroussi and N. Smart (eds). Advances in Elliptic Curve Cryptography , Cambridge University Press, 2005
[11] Cohen H , Gerhard Frey, Handbook of Elliptic and Hyper-elliptic curve Cryptography, Chapman & Hall /CRC, NW, FL, 2006
[12] Enge A , Elliptic Curves and Their Applications to Cryptography: An Introduction, Kluwer Academic Publishers, Norwell, MA, USA,,1999.
[13] Hankerson D, Alfred Menezes, and Scott Vanstone, Guide to Elliptic Curve Cryptography, Springer-Verlag Professional Computing Series, New York, 2004.
[14] Koblitz N , Algebraic aspects of cryptography, Springer-Verlag Professional Computing Series, New York, 1998

[15] Menezes A J, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, Boca Raton, Florida, USA, 1997.
[16] Certicom whitepaper, Remarks on the Security of the Elliptic Curve Cryptosystem.. eptember 1997.