International Journal of Swarm Intelligence and Evolutionary Computation

Darwish and El-Gendy, Int J Swarm Intel Evol Comput 2016, 5:2
DOI: 10.4172/2090-4908.1000135

Research Article Open Access

New Hybrid Cryptosystem for Internet Applications

Ashraf Darwish* and Maged M El-Gendy

Computer Science Department, Faculty of Science, Helwan University, Cairo, Egypt

Abstract

In this paper we demonstrate a new proposed hybrid cryptosystem, which combines the one-time pad that is theoretically unbreakable cipher, with the most strong (standard) encryption algorithms today's, the RSA public-key algorithm, and the AES standard secret-key algorithm, to offer unconditionally secured cryptosystem. Public-key cryptosystem can be used to create a digital signature. The analysis of the proposed scheme shows that with a digital signature, we can be sure the sender and the receiver cannot deny the signed object, and we can ensure the message integrity. The existence of such a system would enable instant secure communication between subscribers who have never met or communicated before. A system of this kind greatly simplifies the problem of key distribution. A one-time pad, under the assumption that it has been exchanged between parties' securely, offers unbreakable cipher! Besides, the proposed scheme facilitates additional level of security strength achieved through the involvement of a four level of key-hierarchy.

Keywords: Cryptography; Hybrid cryptosystem; One-time pad; Internet of things; Cyber security

Introduction and Background

The way to benefit from the advantages of both symmetric and asymmetric cryptosystem has evolved a new approach, the hybrid cryptosystem [1]. The pretty good privacy, PGP, digital envelope cryptosystem is a good example. Threats and vulnerabilities on the communication network and the computing system are monitoring, monitoring modification, masquerading, spoofing and time delay and replay. Network protection services and mechanisms enhances the security of the system and information transfer like confidentiality, authenticity, message integrity, sender nonrepudiation, message unforgiability, access control to system assets during message exchange and availability of the computing system. Cryptography provides basic tools, called primitives, such as encryption, digital signature schemes and hash functions. These primitives can be used with a symmetric-key structure or a public-key structure to achieve our goal. In this paper authors demonstrate the proposed scheme, the exchanged messages format, and the employed four level key-hierarchies

The one-time pad, OTP, cryptosystem is perfectly secure. The major disadvantage of the OTP cryptosystem is the key distribution between the legal entities. Diffie and Hellman solve the problem of the key distribution with the standard Diffie-Hellman key exchange protocol that works without trusted authority. The hard problem behind the strength of their protocol is the Discrete Logarithm Problem (DLP), which opened the world of the public-key cryptography. The Data encryption standard block cipher algorithm, DES, encrypts a plaintext bit string of length 64 using a bit string key of length 56. The key size is too small for current computational power. The need for the advanced encryption standard block cipher algorithm, AES, remained clear that has a flexible key size of 128, 192 or 256 bit string. The public-key cryptosystem can only exist if both one-way and trapdoor one-way functions exist. In this systems two keys are used one to scramble the message, called public key, and one to unscramble the message, called private key. Encryption and decryption keys come in pairs, so that D (E (m, k_p), k_r)=m, where m is the plaintext, the parameter k_r is the private key, and kept with the key holder saved on smart card or e-Token. The parameter k_p is the public key and is distributed to the network participants or stored in a public directory.

In a computer network, data are exchanged between parties through a variety of different types of computing systems. Computer networks offer several advantages, such as resource sharing, increased reliability, distributing workloads, expandability. Currently, all commercial applications are tended to be done through the Internet. Even the office network environment is now extending to employee's home [2]. Generally speaking, any network is subjected to threats and vulnerabilities. Network protection service is a service that enhances the security of the system and information transfer. The service counter the network threats and makes use of one or more protection mechanisms. The protection mechanism is a mechanism that is designed to detect, prevent, or recover from a network threat. The protection mechanisms can support confidentiality, authentication, integrity, nonrepudiation, unforgiability, access control [3] and availability. However, several security problems can be inherent during network access and use. That is why, we are in need to support computer networks with a more powerful and secured cryptosystem [4]. In the proposed hybrid scheme in this paper, which represents an extended version [5] provides confidentiality and authentication that can be used for the Internet sensitive applications and file storage. In the following some algorithms and techniques have been presented.

Truly and cryptographic random bits generators

A number of network security algorithms based on cryptography make use of random numbers, such as the exchanged authentication schemes, session key generation, and generation of keys for the RSA public-key cryptosystem. A key stream generator is defined to be perfect if it is random and unpredictable, or indistinguishable by all polynomial-time statistical tests. The following three criteria are used to validate that a sequence of numbers is random:

***Corresponding author:** Ashraf Darwish, Computer Science Department, Faculty of Science, Helwan University, Cairo, Egypt, Tel: 2025188082, E-mail: ashraf.darwish.eg@ieee.org

Received March 15, 2016; **Accepted** April 26, 2016; **Published** April 29, 2016

Citation: Darwish A, El-Gendy MM (2016) New Hybrid Cryptosystem for Internet Applications. Int J Swarm Intel Evol Comput 5: 135. doi: 10.4172/2090-4908.1000135

1. Uniform distribution**:** The frequency of occurrence of each of the numbers should be approximately the same.
2. Independence**:** No one value in the sequence can be inferred from the others.
3. Unpredictability**:** It means that each number is statistically independent of other numbers in the sequence.

Electrical noise can be turned into a signal, which can switch a gate on, and off, one method of generating random bits by using the zero crossings of this signal to produce pulses, which change the value of single-digit binary counter. For cryptographic applications, it makes some sense to take advantage of the encryption logic available to produce random numbers. Typical examples are the cyclic encryption approach, suggested, and used to generate session keys from a master key. The data encryption standard (DES) algorithm output feedback mode (OFB) can be used for key generation as well as for stream encryption. The standard ANSI X9.17 [6] pseudo random number generator represents one from the strongest CRNGs. PGP hybrid system employs this component.

Hash dunctions and data integrity

A hash function is a computationally efficient function mapping strings of arbitrary length to binary strings of some fixed length, called hash values. If H is a hash function then it is a transformation that takes input m and returns a fixed-size string, which is called the hash value h, that is h = H(m) where h represents the "fingerprint" of a file, or a message. The hash value is appended to the message at the sender. The receiver authenticates that message by re-computing the hash value, and matching it with the received one. To be useful for message authentication, the hash function H should be one-way and collision-free. The output length of the hash code should be substantial. The standard secure hash algorithm (SHA-1) was developed by the National Institute of Standard and Technology (NIST) organization in USA [7] that was published in 1994. The algorithm produces a 160-bit message digest output and more secure against brute-force collision and inversion attacks [8,9]. A problem is called "easy" if we can find a polynomial-time algorithm to solve it and "computationally infeasible" or "hard" if no deterministic or probabilistic polynomial time algorithm is known to solve it.

The OTP cryptosystem

The OTP, fist described by Gilbert Vernam in 1917. In the OTP cryptosystem [10], two copies of one set of the TRNG are generated and distributed over the sender and the receiver. For the strength of the OTP it should fulfill many properties stated [5].

RSA Public Key Cryptosystem

The RSA cryptosystem, named after its inventors Rivest, Shamir, and Adleman, is the most widely used public-key cryptosystem. It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization [11]. RSA encipher a message block $m \in [0, n-1]$ by computing the exponential $c = m^e \bmod n$ where n and e is the key of enciphering transformation and referred to as modulus and encryption exponent. The m is restored by the same operation by using different exponent d or the key, referred to as the decryption exponent, by computing the exponential $m = c^d \bmod n$. The modulus n is the product of two distinct large random primes' p and q then, $n = p.\ q$ and $\phi\ (n) = (p - 1).\ (q - 1)$, where $\phi\ (n)$ is the Euler function. Choose $d > 1$, a large random number, in the interval [Max (p, q) +1, n-1], such that $(d, \phi(n)) = 1$. The two numbers (n, e) constitutes the public encryption key, whereas the remaining items p, q, ϕ (n), and d form the secret trapdoor. The encryption/decryption transformations are based on Euler's generalization of Femat's theorem, which states that for every m relatively prime to n, $m^{\phi(n)} \bmod n = 1$, which implies that if e and d satisfy the relation $e.\ d \bmod \phi\ (n)=1$ and the message $m \in [0, n-1]$ such that gcd (m, n) = 1, then

$(m^e \bmod n)^d \bmod = m.$

By symmetry, enciphering and deciphering are commutative and mutually inverses, thus

$(m^e \bmod n)^d \bmod n = (m^d \bmod n)^e \bmod n = m^{ed} \bmod n = m.$

RSA Digital Signature

The sender creates a digital signature sig by exponentiation $sig = m^d \bmod n$, where d is the sender private key. She sends m and sig to the receiver. To verify the signature, the receiver checks that the message m is recovered $m = sig^e \bmod n$, where e is the sender's public key. In RSA algorithm the p and q parameters must have certain criteria to achieve maximum security for the generated keys, hence ensuring the security of the encryption and decryption processes using these keys.

Calculating the difference between p and q and finding if that difference is less than a given value does checking for closeness of p and q. That value is not a constant value but instead changes when p and q gets larger. The larger the values of p and q the larger that limit must be. So, the checking is done on the "relative difference" of the two numbers. The relative difference is the ratio of the value of the difference between the two numbers, p and q, and the value of the smaller of the two numbers (q). In our proposed system, the relative difference must be larger than 1/128 (0.0078). That is,

$(p - q)/q > 1/128$, $(\delta = p\text{-}q)$, $\delta/q > 1/128$, $\delta > q/128$, $\log_2 (\delta) > \log_2 (q) - 7$.

This condition must be satisfied to ensure that the two numbers are not close together for highly secure parameters p and q.

The Digital Envelope Technique

Although Public-key Cryptosystem [12-14] offer industrial–strong security, it does not mean that secret-key Cryptosystem [12] has gone-off. Public-key cryptosystem are slow in comparison to secret-key cryptosystem, and that is a big concern for anyone who has to send and receive long messages. The Digital envelopes technique is based on the combination of the benefits of both the symmetric and the asymmetric cryptosystem. The strength and the key management of the asymmetric algorithms and the performance and the speed of the symmetric algorithms will also be applied in the hybrid systems. Secret session key of the symmetric algorithm must be used only once, which is recommended, all over the communication. This technique solves the key exchange problem, and the performance. The S-MIME and PGP hybrid cryptosystem are the standard digital envelope technique [15,16]. A number of known attacks exist against PGP. Many of these attacks [17,18] are the brute-force attacks, the private key ring and pass phrase attacks, the public key ring attacks, and the program security.

This paper is organized as follows. Section I introduces general introduction ad some basic algorithms and techniques that can be applied for internet applications. Section II introduces the proposed scheme. Section III discusses the analysis and results of the proposed scheme. Section IV presents the conclusion and future work.

Terminology	Meaning
m, c	The plaintext and ciphertextmessages
OTP_e	The washed One–time Pad
AES^{-1}	AES decryption algorithm
Kid	The 256–bit AES session key
RSA^{-1}	RSA decryption algorithm
KR, KP	The RSA private and public keys
KRA, KPA	The private and public keys of the sender A
KRB, KPB	The private and public keys of the receiver B
SHA	The secure hash algorithm SHA-1
Sig	The signature (message digest encrypted by KRA)
CK	The Kid and the Scheme Pointers encrypted by the KPB
Env	The resulting digital envelope
$Digest_r$, $Digest_g$	The received and generated digest respectively
$+ \oplus$	Concatenation and Vector sum modulo two operation

Table 1: The sending cycle.

The Proposed Unconditionally Secure Hybrid Scheme

The Proposed hybrid scheme provides confidentiality and authentication that can be used for the Internet sensitive applications related to the government activities such as the diplomatic and the military activities and file storage. In the proposed scheme the SHA-1 algorithm to calculate the fingerprint of the message has been used. Table 1 contains the terminology that will be applied.

The combination of the SHA-1 and RSA provides a trusted digital signature scheme. Because of the strength of the RSA, recipient is assured that only the possessor of the matching private key can generate the signature.

In the proposed scheme, the confidentiality is provided by encrypting the massage using the OTP string as a key with a length equal to the message length, using the vector sum modulo two operations. The receiver has the same copy of the OTP that he can use it to decrypt the received message after applying the washing process on the OTP key portion. The AES session key is recovered by the RSA receiver's private key after striping it off from the message then used it in the washing process.

Confidentiality and authentication can be applied to the same message. First, the signature of a message m is generated and appended to the message m. The OTP key is selected and washed using AES algorithm. Both the message and the signature together are encrypted with OTP_e using the vector sum modulo two operations to generate the encrypted message c. The session key, kid, and the OTP pointer are encrypted using RSA and sent with c in a special formatting. The formulation of the confidentiality and the authentication are as follows (Table 1).

(a) The sending cycle

1. Washing Process:

$$OTPe = AES_{kid} [OTP]$$

2. Key exchange Process:

$$CK = RSA_{KPB} [kid + Pointers]$$

3. Digital Envelope Process

$$Sig = RSA_{KRA} (SHA [m]),$$

$$MT = m + sig$$

$$C = OTP_e \oplus MT = OTP_e \oplus [m+sig]$$

$$OTP_e \oplus(m + RSA_{KRA} (SHA [m]))$$

$$Env = c + CK$$

(b) The receiving cycle

1. Session key Extraction Process:

$$Kid = RSA^{-1}{}_{KRB} [CK]]$$

2. Washing Process:

$$OTPe = AES_{kid} [OTP]$$

3. Digital Envelope Opening Process:

$$MT = c \oplus OTP_e = (OTPe \oplus (m + sig)) \oplus OTPe$$

$$m + sig= m+ RSA_{KRA} (SHA [m])$$

$$Digestg = SHA [m] \ldots \text{generated by the receiver}$$

$$Digestr = RSA^{-1}{}_{KPA} [sig]$$

$$RSA^{-1}{}_{KPA} (RSA_{KRA} [SHA[m])= SHA [m].$$

Then, the two fingerprints, $Digest_g$ and the $Digest_r$, are compared for matching to validate the sender and the integration of the received message. Before using OTP to encrypt the message, the OTP string is encrypted through the washing process using AES algorithm with a random 256–bit session key. Each OTP key and session key is used only once for each massage. To protect the used session key, it is encrypted with the RSA receiver's public key, and sent together with the encrypted massage.

Results and Analysis of the Proposed Scheme

The strength of AES algorithm or the strength of RSA algorithm does not bound the security of the scheme. The strength of RSA is proved. The RSA attack, the factoring problem, seems to be effective due to the increase in processing speeds in today's computing systems. Increasing the length of the RSA parameters can cover this attack. In our scheme, we implement the RSA algorithm with variable key lengths parameters that can deal with length up to 8192 bits.

The AES algorithm is a 128-bit iterative block cipher with a 256-bit key and fourteen rounds. The security of AES algorithm relies on the use of three incompatible types of arithmetic operations on 32-bit words. One of the principles during the design of AES was to facilitate analysis of its strength against differential cryptanalysis. AES is considered to be immune from differential cryptanalysis [19]. In addition, no linear cryptanalytic attacks on AES have been reported and there is no known algebraic weakness in AES. The strength of AES is also guaranteed through the use of a session key only once per message. A 256-bit key seems to be reasonable enough.

If we assume, in the worst case, that the session key has been compromised, then we still have the OTP, which is exchanged, securely between our extranet subscribers. On the other hand, the vector sum modulo two operation employed is fast enough that it does not add any overhead or effect the performance of the scheme. As a conclusion, the OTP provides the security of the scheme if AES or RSA keys have been compromised. On the other hand, if the OTP has been compromised the RSA and AES can guarantee the security of the scheme because we apply the washing process on the used OTP portion before the message encryption process. The scheme employs the SHA-1 to generate the message fingerprint. It provides 160-bit message digest. It is very hard to lie under the Birthday attack.

Conclusion and Future Work

As of today, a lot of applications have been done through the Internet. Electronic mail provides a low cost means of communicating with customers, suppliers, and partners. The Internet greatly simplifies the task of providing information to citizens, clients, suppliers, and partners, or at least those that have computers connected to the Internet. Any use of electronic information publishing reduces the number of requests for information via telephone or mail. Doing research over the Internet generally involves using client software to search for retrieve information from remote servers. Types of client software include File Transfer Protocol (FTP) software that supports logging into remote system, browsing directory structures, and retrieving files. The electronic commerce, the electronic funds transfer, e-Voting election schemes and the future applications related to Internet of Things (IOT) are other important Internet applications. Currently, all commercial applications are tended to be done through the Internet. Even the office network environment is now extending to employee's home.

The Security is the key consideration since a single security incident can wipe-out any cost savings or revenue provided by Internet connectivity. On the other hand encryption algorithms that could need long time to break in the near past, today's it may be broken in shorter time, due to the fast progress in software and hardware technology. That is why we are in need to design new techniques that are considered to be very hard to break.

References

1. Gupta RK, Singh P (2013) A New Way to Design and Implementation of Hybrid Crypto System for Security of the Information in Public Network. International Journal of Emerging Technology and Advanced Engineering 3: 8.
2. Arbaugh WA, Davin JR, Farber JD, Smith MJ (1998) Security for Virtual Private Intranets. Univerity of Pennsylvania IEEE.
3. Ellison CM (1999) Intel Security Technology Lab. The nature of a usable PKI Computer Networks.
4. ElGendy MM, Dakroury YH, El-Hennawy ME, Amer FA (2000) The Digital Envelope Techniques and the Internet Security. The Proceedings of the Egyption Informatics Journal 1: 26-44.
5. Stalling W (1995) Network and Internetwork Security Printic Hall.
6. National Institute of Standards and Technology (1994) Announcement of Weakness in the Secure Hash Standard.
7. Robshaw MJB (1995) MD2, MD4, MD5, SHA and Other Hash Functions. Technical Report TR-101 version 4.0. RSA Laboratories.
8. Preneel B (1993) Analysis and Design of Cryptographic Hash Functions, Ph.D. Thesis. Katholieke University Leuven.
9. Dorothy E, Denning R (1983) Purdue University, Cryptography and Data Security. Addison-Wesley Publishing Company.
10. Diffie W, Hellman M (1975) new directions in cryptography, IEEE Trans. On Inform Theory IT 22: 329-340.
11. Alexander M (1996) The Understanding Guide to Computer Security. Addison-Wesely Publishing Company.
12. Brassard G (1988) Lecture Notes in Computer Science Modern Cryptology.
13. Goos G, Hatmanis (1988) Modern Cryptology, A Tutorial, Lecture Notes in Computer Science. Springer-Verlag.
14. Atkins D, Buis P, Hare C, Kelly R, Nachenberg C, et al. (1997) Internet Security, Professional Reference. New Riders Publishing. Indianapolis IN.
15. Yao A (1982) Theory and applications of trapdoor functions, In Proc. Of the 23rd Annual IEEE Foundation Computer Science. IEEE New York pp: 80-91.
16. Daemen J, Govaerts R, Vandewalle J (1994) Weak keys for IDEA in Advances in Cryptology Crypto. Springer-Verlag 93: 224-231.
17. Lai X, Massey JL, Markov SM (1992) Ciphers and differential cryptanalysis, In Advances in Cryptology Eurocrypt. Springer bVerlag 91: 17-38.
18. National Institute of Standards and Technology (1993). FIPS Publication 180, Secure Hash Standard (SHS).
19. Aravindhu N, Venkatesan G, Anandhanayagie IS (2014) Data Sharing in Cloud Using Hybrid Cryptosystem. International Journal of Advanced Research in Computer Science and Technology 2: 1.

Citation: Darwish A, El-Gendy MM (2016) New Hybrid Cryptosystem for Internet Applications. Int J Swarm Intel Evol Comput 5: 135. doi: 10.4172/2090-4908.1000135