Improved Security with Signcryption

Prof. S. A. Jain*, Ms. Ashwini B. Abhale,Mr. Amol S. Jadhav****

*Research Scholar Dept. of Computer engineering, Maharashtra Academy of Engineering, (Alandi) University of Pune, India.

**Research Associate, Dept. of Computer engineering, Maharashtra Academy of Engineering, (Alandi) University of Pune, India

Abstract— Signcryption is a new cryptographic primitive, which simultaneously provides both confidentiality and authenticity. Previously, these two goals had been considered separately, with encryption scheme provide confidentiality and digital signature provides authenticity. In cases where both required, the encryption operations and digital signature operations were simply sequentially composed. Zheng's demonstrated that by combining both goals into a single primitive it is possible to achieve significant savings both in computational and communication overhead. In this work our main Objective was to implement and compare Zheng's signcryption algorithm with signature-then-encryption and encryption-then-signature technique for any type of files such as txt, pdf, doc, audio, video etc and investigate the time delay for above mentioned three methods.

Introduction

Digital signature is used for authentication and ensures non-repudiation. Non-repudiation prevents either sender or receiver from denying a transmitted message. When a message is sent, the receiver can prove that the alleged sender in fact sent the message. When the message is received, the sender can prove that the alleged receiver in fact received the message.

To enforce the attribute of security such as confidentiality, authenticity, unforgeability and non-repudiation the message is first signed and then encrypted or vice-versa. This approach is known as signature-then-encryption. The main disadvantage of this approach is that, digitally signing message and then encrypting it, consumes more machine cycles and bloats the message by introducing extended bits to it. Hence, decrypting and verifying the message at the receiver's end, a lot of computational power is used up. Thus you can say that the cost of delivering a message using signing-then-encryption is in effect the sum of the costs of both digital signatures and public key encryptions

Signcryption is a new paradigm in public key cryptography that simultaneously fulfils both the functions of digital signature and public key encryption in a logically single step, and with a cost significantly lower than that required by the traditional signature followed by encryption.

In order to send a confidential message in a way that it cannot be forged, it has been a common practice for the sender of the message to encrypt message by public key or secret key cryptography and then send it. This only ensures confidentiality and unforgeability. If there is active attack on encrypted message such as masquerade, replay or modification of message the receiver will not know this. In order to beware of such attack receiver must ensure security features such as authentication and non-repudiation.

I. SIGNCRYPTION ALGORRITHM

The original signcryption algorithm is based on the shortened DSS. The parameters are the same As those used in the shortened DSS, and the difference between the signcryption scheme and the shortened DSS lies in the fact that the signcryption scheme provides both signature and encryption

A. Signcryption algorithm

Parameters

P: a large prime number.
q: a prime number which divides -1.
g : an element in Zp with order q modulo p
m : message.
$E_k(m)$: symmetric encryption algorithm with secret key k.
$D_k(m)$: symmetric decryption algorithm with secret key k
Hash : a one-way hash function
KH_k : a keyed one-way hash function with key k`
xa : sender's private key, randomly chosen from 1<=xa<=q-1
ya : sender's public key, ya = g^{xa}(mod p).
xb : receiver's private key randomly chosen from 1<=xb<=q-1
yb : receiver's public key, yb = g^{xb}(mod p)

Sender's Signcryption

1. Select x uniformly and randomly from 1<=x<=q-1.
2. Calculate k = hash (yb^{x} (mod p)).
3. Split k into k1 and k2 of appropriate length.
4. Calculate r = KH_{k2}(m).
5. s = x /(r + xa) .(mod q) : SCS1
   s = x /(1 + xa .r) (mod q) :SCS2
6. c = E_{k1} (m).
7. Send the signcrypted text (c ; r ; s).

Receiver's Unsigncryption

1. Recover k using r; s,g, p; q; ya; xb.
   k = hash ($(ya.\ g^{r})^{s.xb}$ (mod p)) :SCS1
   k = hash ($(ya^{r}.\ g)^{s\ .xb}$(mod p)) :SCS2
2. Split k into k1 and k2.
3. m = D_{k1} (c).
4. Calculate KH_{k2}(m) and accept m as valid message if KH_{k2}(m) = r.

B. Step's involved in signcryption

We are taking an example in which Alice is sender and bob is receiver. So Alice is having a message m, which wants to send to bob in an unsecured channel, hence he uses signcryption mechanism to send the message to bob so tat message would remain safe. So below steps are discussed which are involved in Signcrypting the message.

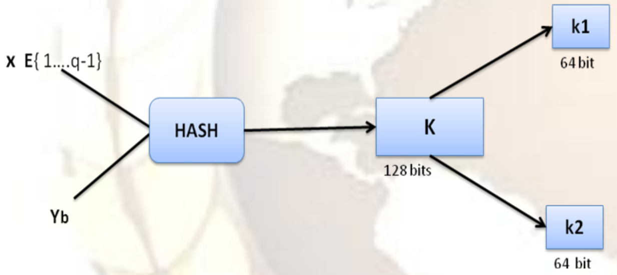
1. Alice chooses a value x from the large range 1,…,q-1

2. She then uses Bob's public key and the value x and computes the hash of it.

This will give her a 128-bit string. K = hash (ybx mod p)

3. She then splits this 128-bit value K into two 64-bit halves. We can name them as

k1 and k2 and refer to them as the key pair.



4. Next, Alice encrypts the message m using a public key encryption scheme E with the key k1. This will give her the cipher text c. c = E k1 (m)

5. Then, she uses the key k2 in the one-way keyed hash function KH to get a hash of the message m. This will give her a 128-bit hash, which we will call r. This process uses the SDSS Algorithm. r = KH k2 (m).

6. Just like in SDSS, Alice then computes the value of s. She does this using the value of x, her private key xa, the large prime number q and the value of r. s = x / (r + xa)mod q

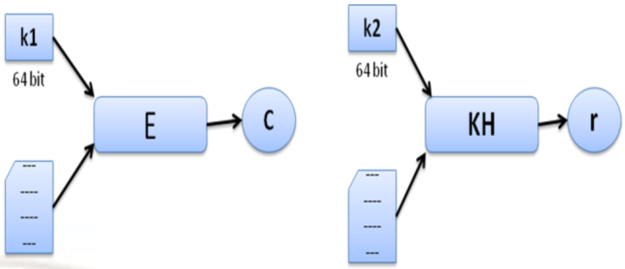


Fig. Signcryption - generating components c and r

7. Alice now has three different values, c, r and s. She then has to get these three values to Bob in order to complete the transaction. She can do this in a couple of ways. She can send them all at one time. She can also send them at separately using secure transmission channels, which would increase security. Thus on her part, Signcryption of the message is done.

C. Steps involved in Unsigncrypting a message

1. Bob receives the 3 values that Alice has sent him, c, r and s. He uses the values of r and s, his private key xb, Alice's public key ya and p and g to compute a hash which would give him 128-bit result.

K = hash ((ya * gr)s X xb mod p)

This 128-bit hash result is then split into two 64-bit halves which would give him a key pair (k1,k2). This key pair would be identical to the key pair that was generated while Signcrypting the message.

2. Bob then uses the key, k1, to decrypt the cipher text c, which will give him the message m.

m = Dk1(c)

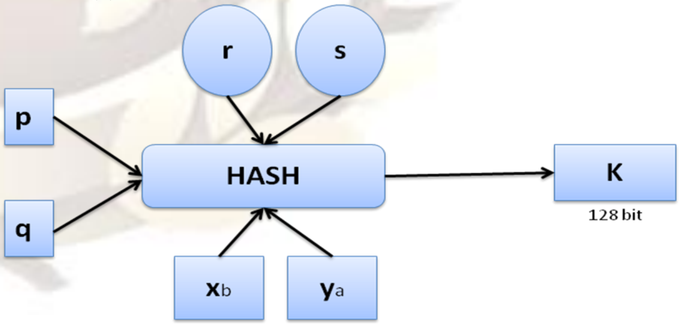


Fig. Unsigncryption – obtaining component K

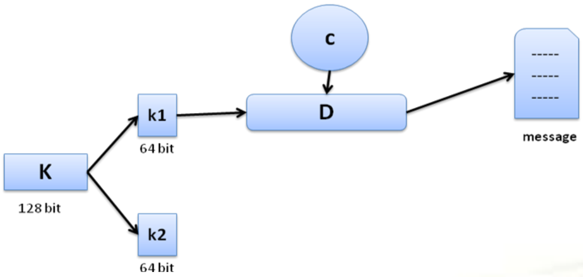


Fig: Unsigncryption – obtaining the message m

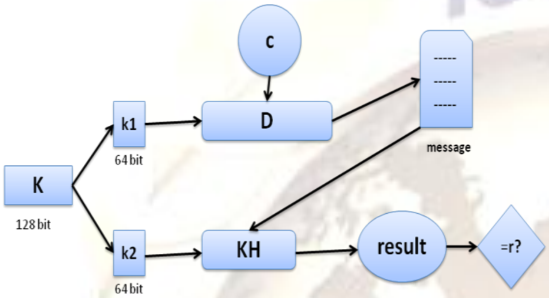


Fig Unsigncryption – verification of the message m

II. Features and Security Aspects of Signccryption

A. *Features*

Digital signcryption strives to do digital signature and public key encryption in one logical step, with a cost less than that required by each of those steps done separately. Let us assume S is signcryption algorithm and U is the unsigncryption algorithm.

The following three aspects define the features of signcryption:-

a. **Unique unsigncryptability:-**

A message m of arbitrary length is signcypted using the algorithm S. This will give signcrypted output c. The receiver can apply unsigncryption on c to verify the message m. This unsigncryption is unique to the message m and sender.

b. **Security**

Since signcryption is a combination of two security schemes, digital signature as well as public key encryption, it is likely to be more secure and would ensure that the message sent couldn't be forged, the contents of which are confidential and ensure non-repudiation.

c. **Efficiency**

The cost of computation involved when applying the signcryption and unsigncryption algorithms as well as the communication overhead is much smaller than with signature-then-encryption schemes.

B. *Security*

a. **Unforgeability**

Bob is in the best position to be able to forge any signcrypted message from alice as only he is in possession of his private key, xb, which is required to directly verify alice's message. Given the signcrypted text of c, r, s, bob can only obtain the message m by decrypting it using his private key xb. Any changes he then makes to the message m will reflect in the next step of signcryption, which will ensure that the one way keyed hash function on the message m, will not will not match the value r. Thus bob, the prime candidate for this kind of attack, is prevented from forging alice's signcrypted message.

b. **Confidentiality**

Given that an attacker has obtained all three components of the signcrypted message, c, r and s, he still would not be able to get any partial information of the message m because he would have to also know bob's private key as well as the two large prime numbers p and its factorial q,known only to bob and alice . This is not feasible , as we know that deriving a factorial from a large prime number is not possible

C. *Comparisons:-*

The advantage of signcryption over signature-then-encryption lies in the dramatic reduction of computational cost and communication overhead, which can be symbolized by the following inequality:
Cost (signcryption) < Cost (signature) + Cost(encryption)

III. CONCLUSION

Signcryption is a very novel idea that, if implemented in the right way, can be very useful in network security domain.

In life, it is human nature to try and do two things at once, or to **'kill two birds in one stone'.** Humans do this to make shortcuts, save on time and resources.. Is this best approach to do things? In terms of computer security, like we explained before, we believe that by combining two complex mathematical functions, you will increase the complexity and in turn increase security. Signcryption still has a long way to go before it can be implemented effectively and research is still going on in various parts of the world to try to come with a much more effective way of implementing this.

IV. References

[1] J.Baek, R.Steinfeld and Y.Zheng. Formal Proofs for the Security of Signcryption. Journal of Cryptology, 2007, 20(2): 203-235

[2] Y.Desmedt. Society and Group Oriented Cryptography. Advances in Cryptology-Crypto'87. Berlin: Springer-Verlag. (1988) 120-127

[3] Van Der Merwe J, Dawoud D, McDonald S. A survey on peer-to-peer key management for mobile ad hoc networks. ACM Computing Survey. 2007, 39(1):1-45

[4] R.Gennaro, S.Jarecki, H.Krawczyk, T.Rabin. Robust Threshold DSS Signatures. Information and Computation. 2001, 164(1): 84-101

[5] Y.Han. Generalization of signcryption for resources-constrained environments. Wireless Communications and Mobile Computing, 2007, 7(7): 919-931

[6] Y.Han, X.Yang, Verifiable Threshold Cryptosystems based on Elliptic Curve, Proceedings of International Conference on Computer Network and Mobil Computing, IEEE Press, (2003)334-337

[7] H.Krawczyk, The Order of Encryption and Authentication for Protecting Communications (or: How secure is SSL?), In Advances in Cryptoloty- Crypto'01, Lecture Notes in Computer Science, Vol.2139. Berlin: Springer-Verlag, (2001) 310-331

[8] S.K.Langford. Threshold Dss Signatures without a Trusted Party.Lecture Notes in Computer Science, Vol.963, Berlin: Springer-Verlag. (1995)397-409.

[9] T.P.Pedersen. A threshold cryptosystem without a trusted party. In Advances in Cryptology-Eurocrypt'91, Lecture Notes in Computer Science, Vol.547. Berlin: Springer-Verlag, 1991.

[10] A.Shamir, How to share a secret. Commun. ACM, vol. 22, pp.612–613, 1979.

[11] Y.Zheng, Digital signcryption or how to achieve cost (signature &encryption) << cost (signature) + cost (encryption), (Extended abstract), In Advances in Cryptoloty-Crypto'97, Lecture Notes in Computer Science, Vol.1294, Berlin: Springer-Verlag. (1997) 165-179.