Volume 4, Issue 9, September 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Modern Methods of Encryption: Tendencies and Challenges

Vishal M. Shah[1], Viral V. Kapadia[2]
[1]Computer Engineering Department,Sardar Vallabhbhai Patel InstituteTechnology, Vasad, India
[2]Computer Science & Engineering Department, The M. S. University, Baroda, India

Abstract— numeroustechniques of encryption are available for information secrecy and therefore,this paper describes advance encryption techniques for users. Also, a review on Secrete-key Encryption, Public-key Encryption, Identity-Based Encryption and a more commonidea of Attribute-Based encryption are explained in details. In this paper, we show comparison of different encryption methods and also the evolutionary path of encryption methods which are also described for commonresponsiveness to the users.

Keywords— Secrete-Key Encryption, Public-key Encryption, Identity-Based Encryption (IBE), Attribute-based Encryption (ABE), and Key Generation Centre (KGC)

I. INTRODUCTION

People are anxious with Secrecy of information since ancient times. Encryption methodsconvert data into an unreadable form to ensure secrecy of data [1].One of the vitalfacets of security is confidentiality which can be achieved through different encryption technology. The general categorization of encryption techniques based on keys are private/secrete or public key encryption/cryptography. The new tendencies in encryption are identity-based cryptography and attribute-based cryptography.

Getting started from Secrete-key Encryption, encryption i.e. converting the message into cipher-text and decryption means converting thecipher-text into message – reverse of encryption, algorithm of all the cryptosystems provide same key. It means that the encryption key- E_k, held by the principal who encrypts a message, anddecryption key-D_k, held by the one who will get the cipher-text and decrypt it, are same. This is called as Symmetric-Key cryptosystems [1]. In this cryptosystem, a previous shared secret should be established by an authenticated and private communications channel before a cryptosystem can be used. Due to difficulties in distributing a secrete keys [1], there is another protocol came into existence which was proposed by Diffie-Hellman. This protocol [2] was shared secrete-key over public channel without using any prior secrete. Eavesdroppers can still read the transcripts generated during the execution ofthe protocol, but cannot derivate the session key that the protocol participants compute locally and secretly [1]. The protocol is now known as Diffie-Hellman key exchange. Later, Diffie-Hellman and Merkle key exchange [3] together proposed Public-key Encryption technique in which E_k and D_k are different and E_k was available publicly. Public-key cryptosystems are also known as asymmetric cryptosystems.

In Public-Key Encryption, the public key is a usually string which hasn't any relation with owner's identity and so one can resort to key exchange protocol(like Diffie-Hellman) to have a confidential communication channel in case of authenticated channels are available and message recipients are online [1]. But in network like Internet which is not secured, it isn't clear who is owner of the key. And for individual, authenticating process is very difficult all other parties over the network and therefore, with use of PKI-Public key Infrastructure, the trust is maintained. In PKI, a trusted-by-all party called certificate authority (CA) provides a digital certificate to each entity, which may be an individual or an organization [1]. By the help of certificate, the CA certifies the relationship between an identity and a public key. Because there are many difficulties, PKI is not adopted as widely as hoped. And so in 1984, Shamir [4] proposed a new encryption scheme which is called Identity based Encryption (IDE) which solves public key distribution. The feature that differentiates IDE with any other Public-key encryption technique is the way a public and private key pair is set up. KGC – Key Generation Center is liable for the private key generation after user authentications. The major benefit of this approach is to largely reduce the need for processing and storage of public key certificates under traditional PKI [1].

Due to strict nature of IBE with respect to some error tolerance such as noisy biometric measurements as identities is desirable; Sahai and Waters proposed [5] a new fuzzy based IBE scheme which is used to support Attribute based Encryption technique in which some set of attributes are shared by set of entities. For both biometric applications and access control applications, it is essential for an ABE scheme to have collusion resistance, which guarantees that two colluding userscannot pool their keys to decrypt a message that they are not allowed to.

II. RELATED WORK

A. Symmetric Key Cryptography

Symmetric key cryptosystem was the first and oldest encryption technique back in 1970s which was based on dedicated key management architecture uses the same data encryption technology to manage keys and scramble data. In

this system, the same key is used to encrypt and decrypt information and the key manager generates a new key for every message at the sender's request. The key is stored in a database along with the list of receivers. When the receiver authenticates, the key is retrieved from the database and the receiver name is matched against the list of authorized recipients. As in the Fig.1 shows Symmetric Key Cryptographic system in which the same key K is used for encryption and decryption process. Symmetric key systems have become the centrepiece of internal-only encryption and authentication systems. But Symmetric key crypto-System has few disadvantage as it has high storage cost and high availability needs.

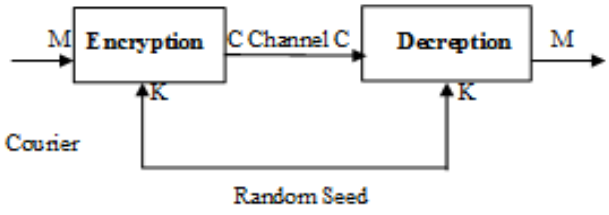

Fig. 1 Secrete-key Cryptography
[M – Plaintext (Message), C- Cipher text, K – secrete key]

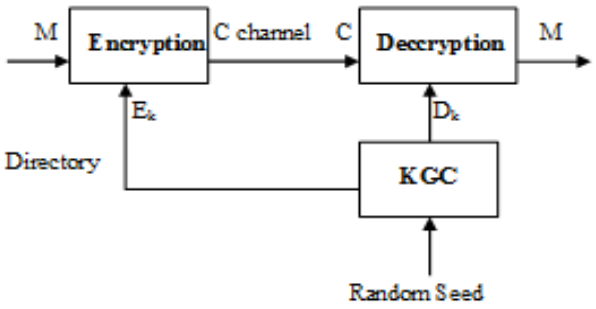

Fig. 2 Public-key Cryptography
[M – Plaintext (Message), C- Cipher text, KGC – Key Generation Center, E_k – Encryption key, D_k – decryption key]

B. Public Key Cryptography

Asequences of mathematical innovations led to important new kinds of encryption algorithms in early 80's. These algorithms, called "public key" or "asymmetric" systems use a separate key to encrypt data than the one they use to decrypt data. The famous Diffie-Hellman [2] and RSA algorithms are the best-known examples of public key algorithms. Public Key Cryptosystem which is also called Asymmetric Key management in which two keys E_k and D_k are keys used for encryption and decryption respectively, is described in Fig. 2. Trusted third party deliverthese keys which is called as KGC – Key Generation Center. In this method, one key is public key and other is private key. This method is quite useful as far as securely encryption and decryption are concerned as there is no previouslymutual key is required as in Symmetric key encryption approach. But it has some downsides as well. The public key is assigned by the KGC to the user is actually any random string which is not related at all to the user. This does not give any information about user's identity in case of forgery. This problem has given birth to Identity-Based encryption which is a novel technology in cryptography.

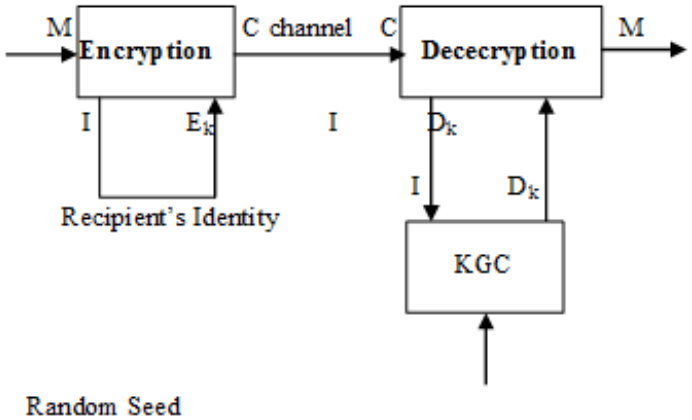

Fig. 3 Identity-Based Cryptography
[M – Plaintext (Message), C- Ciphertext, KGC – Key Generation Center, E_k – Encryption key, D_k – decryption key, I- Identity of the user]

C. Identity-Based Cryptography

Adi Shamir [4], proposed a new type of public key algorithm in 1984. While public key systems have the inherent problem of distributing public keys and tying those public keys to a specific receiver, Shamir proposed mathematically generating the receiver's public key from his/her identity, then having the key server calculate the required private key. This system is called an Identity-Based Encryption (IBE) algorithm. This approach would remove the need for public key queries or certificates. Because the key server generates the private key – based on identity of user, key recovery no longer requires a separate private key database. For example, when user Xwants to send a message to user Y, he signs it with the secret key in his smart card, encrypts the result by using Y's name and network address, adds his own name PAN number to the message, and sends it to Y. When Y receives the message, he decrypts it using the secret key in his smart card, and then verifies the signature by using the sender's name and PAN number as a verification key.

Fig. 3 demonstrates working of IBE in which both encryption and decryption are associated with same identity (I) of the user.

Identity-Based Encryption technique is very useful compared to traditional approaches described above two approaches. But as in IBE there is identity associated with the public key and Ciphertext and the nature of IBE with respect to some error tolerance such as noisy biometric measurements as identities is strict. So this is disadvantage in using IBE technique.

D. Attribute – Based Cryptography

People are identified by their attributes. ABE is actually a generalization of identity based encryption [1]. Sahai and waters [5] proposed a system in which a sender can encrypt a message specifying an attribute set and a number d, such that only a recipient with at least d of the given attributes can decrypt the message. There are two structures available in ABE scheme:

1) Key policy attribute-Based Encryption (KP-ABE) [9] and
2) Ciphertext policy Attribute based Encryption (CP-ABE) [8].

Goyal et al. [6] proposed a KP-ABE scheme which supports any monotonic access formula consisting of AND, OR, or threshold gates. This scheme is characterized as key-policy ABE since the access structure is specified in the private key, while the attributes are used to describe the Ciphertext.

The roles of the Ciphertext and keys are reversed in the Ciphertext policy ABE (CP-ABE) introduced by Bethencourt, Sahai and Waters [7], in which the Ciphertext is encrypted with an access policy chosen by an encryptor but a key is simply created with respect to an attributes set.

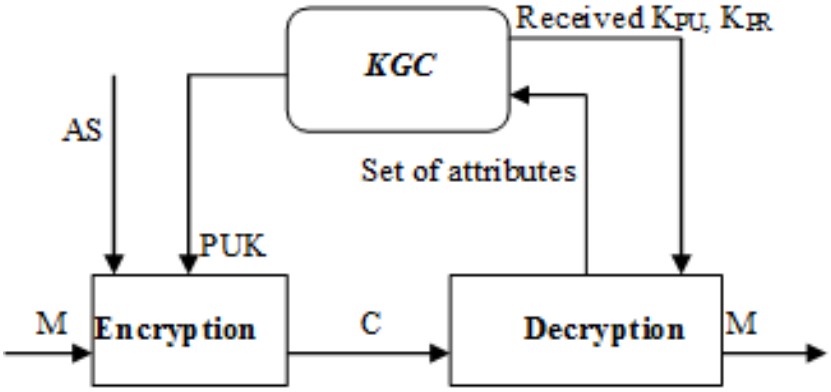

Fig. 4 Attribute-Based Encryption

[K_{PU} – Public key, K_{PR} – Private Key, AS – Access Structure, KGC – Key Generation Center, M – Message, C – Ciphertext]

Fig. 4 is the attribute-based encryption approach in which during the encryption access structure and public key (K_{PU}) are used to encrypt the message and then Ciphertext along with the set of attributes are used to decrypt the message.

III. COMPARATIVE ANALYSIS

We have shown different encryption techniques such as Public-key cryptography, IBE, ABE and we have shown how they are differing from each other. In this section we have shown comparative analysis with respect to criteria such as number of keys in network, non-repudiation, digital signature, key directory and availability of encryption keys as shown in TABLE 1 [8]. As far as number of keys in network is concerned all of above techniques perform almost equally well but it is differed in terms of how it supports non-repudiation, digital signature, key directory and availability of encryption keys which is shown in table 1.

As shown in table 1 attribute-based cryptography supports ABE scheme which differs from public-key and identity-based cryptography. Same way, Identity-based cryptography doesn't support ABE scheme as shown in table 1.

TABLE 1 COMPARISON OF DIFFERENT ENCRYPTION SCHEMES [8]

	Public-key Cryptography	Identity-Based Cryptography	Attribute-Based Cryptography
No. of Keys in Network	O(n)	O(n)	O(n)
Digital Signature, Non-Repudiation	YES	YES	NO
Availability of encryption key	NO	YES	NO
Key Directory	YES	NO	NO

IV. CONCLUSIONS

In this paper, we have shown different encryption approaches such as Secrete-Key cryptography, public-key cryptography, identity-based cryptography and attribute-based cryptography. Along with this, we have shown performance comparison with respect to some criteria such as number of keys in network, digital signature, non-repudiation, availability of encryption key, etc. which is shown in table 1.

REFERENCES

[1] Sze – Ming Chow, "New Privacy preserving Architecture for Identity -/ Attribute-based Encryption",Department of Computer Science, Courant Institute of Mathematical Sciences, New York University, September 2010.

[2] D. Whitefield and M.E.Hellman,"New Direction in Cryptographic", IEEE Transactions on Information Theory, vol. IT.22, no. 6, November 1976.

[3] R. C. Merkle, Secure Communications over Insecure Channels, Communications of the Association for Computing Machinery, 21, 294–299, 1978.

[4] A. Shamir, "Identity-Based cryptosystems and signature schemes", "CRYPTO", Springer, 1984.

[5] A. Sahai and B. Waters, "Fuzzy Identity-based Encryption", Volume 3943 of LNCS pp 457-473, Springer, 2005.

[6] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data", Association for Computing Machinery, 2006.

[7] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption", pp 321-334, 2007.

[8] H. Seo, C. Kim and H. Kim, "Using attribute-Based Cryptography", IEEE-2011.

[9] C. Wang and Y. Liu, "A Secure and Efficient Key Policy Attribute-BasedEncryption Scheme", IEEE, 2009.

