SECURED DIGITAL COMMUNICATION TECHNIQUES FOR DATA DISTRIBUTION OF SEAWATCH INDONESIA

Michael A. Purwoadi*

Abstract

In this paper, several secured digital communication techniques will be described. According to the nature of communication between data-base of Seawatch Indonesia and its users, a protocol involving hybrid cryptosystem and digital signature techniques seems to be the most preferred among the others. The protocol will provide faster algorithm process than ordinary public-key technique and can circumvents the eavesdropper located in the middle of channel. It allows the use of widely available internet network.

I. INTRODUCTION

Seawatch Indonesia collects marine data such that temperature, sea-current direction, tidal by its sea-buoy stations. They will be redistributed for research purposes, economic mission or public utility such climate forecasting, tidal and sea-current prediction conducted by government or private institutions. In some cases, data or information (data that has been already processed) is confidential because it has an economic value or a defense interest. If the information or data is fallen into non-desired persons, it could cause an enormous economic lost, or even bigger accident. The easiest solution is to use a dedicated communication channel such that a dedicated least-line. This solution is very expensive

With this solution, there will be no intruder between the sender and the receiver. Unfortunately this solution costs very expensive, especially when the transfer of data needed is sporadic, say once a day or once a week. The solution costs even more if we have to install a new hardware such telephone wire. So we look for another solution that can optimize the use of communication channel and that can still guarantee these qualities below :

1. Confidentiality
2. Integrity
3. Authentication
4. Nonrepudiation of demand

* Directorate for Electronics and Information Technology – TIEML – BPPT

In other part, the internet network is already widely available. Almost every research institution and government office has been connected to it. They use it for searching and exchanging information. Then, it is interesting to use also the internet as communication channel to distribute data / information from Seawatch Indonesia's database center to its clients.

II. INTERNET AND DATA DISTRIBUTION CHARACTERISTICS OF SEAWATCH INDONESIA

Main characteristics of internet network are packets, routing and broadcasting. It means that information is divided into several packets of bits stream, usually 1.5 kilobytes, labeled containing destination address before sending. The packet, when it comes into the network, is received by several routers. Among them, only ones that are configured will retransmit the packets to other routers. It is repeated until the packets reach its destination.

So, data sent from database center will pass through several routers before arriving to its destination. An intruder can take position near a appropriate one and catches the data demanded by user. Usually, users will ask to Seawatch Indonesia for sending them some data. The demand from users itself, don't need to be hidden, but the data that they want, must be protected because of its economics value from undesired eavesdropper.

It is quite different from what is done in the internet secured communication nowadays. Using secured socket layer (SSL), internet provides a security the data that user sends to a Web Server. The data could be credit card number, social security number or others. It is encrypted such that only the server can decrypt the packet and extracts the information. As mentioned above, for data distribution of Seawatch Indonesia an inversed procedure is needed, i.e. the data from database center / server must be encrypted such that only the demanding user can decrypt and extract the data.

III. SECURED DIGITAL COMMUNICATION AND HYBRID CRYTOSYSTEM.

A secured digital communication is based on a crypthography algorithm i.e. the mathematical function used for encryption and decryption. For long ago, the secret of this algorithm provided the security. Only ones that know the algorithm can decrypt the packet.

Denoting the information is I, crypted data is C, encryption algorithm as E and decryption algorithm as D, so we have :

$$C = E (I)$$
$$I = D (C)$$

Nowadays, the cryptosystem combines algorithm and a code called key K, such we have

$$C = E_K (I)$$
$$I = D_K (I)$$

By this way, the algorithms can be published but the key K is still remained secret. We can use the "on-the-shelf" algorithm, and this method allows a standardization of the algorithm. The techniques is called symmetric cryptography because both parts use the same key.

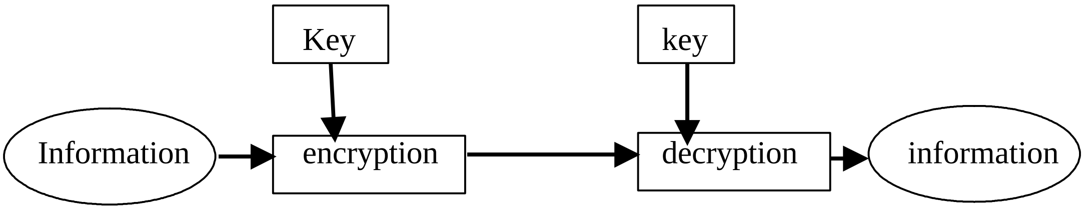

Figure 1. *Symmetric algorithm*

However, this technique has a major inconvenient concerning transmission of the key from database center to client. It must not be sent before assuring that the communication channel is safe. It is also not convenient if we want to change the key for each transaction. This problem is known as key-management problem.

In 1976, a new concept was proposed introducing a public-key and private-key. This cryptosystem uses two different keys, one public and other private. It is very hard to compute the private key from the public key. In this technique, anyone can have the public key and can encrypt the data but not decrypt it. Only the person with private key can decrypt the message.

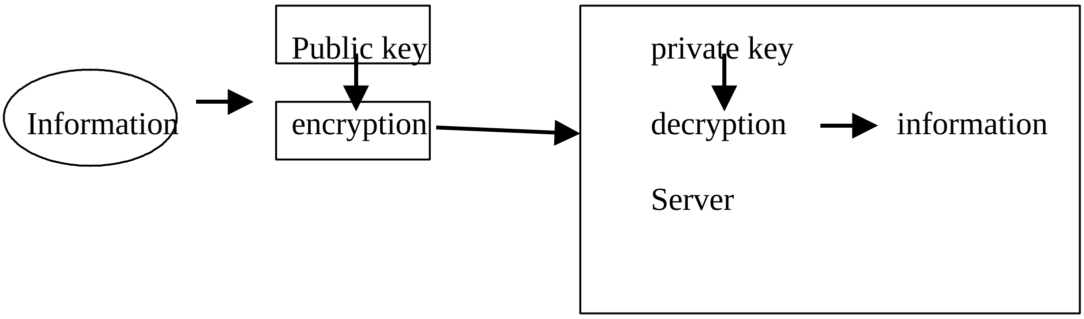

Figure 2.: *Public-key algorithm*

With this technique, the server can send its public key to everyone. Two of its client can not communicate using the key because neither has the private key. By this way, the problem of key-management can be resolved and the communication from client to its server can be realized. This is the way that the secured communication in internet is implemented. As mentioned above, some modification is needed because of the different direction of data that must be encrypted. This modification will be explained below as the hybrid cryptosystem because it uses both symmetric and public-key cryptosystem.

IV. HYBRID CRYPTOSYSTEM

Usually, public key cryptosystem is much slower than symmetric algorithm such that it is not used for encrypt the information; it is used to encrypt key. The server send a public key to its client, the client generates its symmetric key K, encrypts it using public key and then, send it to the server. The server decrypts the data and obtains the key K using its private key. Now, client and server can communicate using the agreed key K.

The protocol for the communication between database server of Seawatch Indonesia and its user can be listed below :

1. User sends a message to server asking for a connection
2. Server sends its public key
3. User generate a random key K, encrypts it using server's public key, and sends it to the server
4. Server decrypts client's message using its private key to recover the key K
5. Both of them encrypt their communication using the same session key

For better security, the procedure above can be initiated for each transaction, such that the key K is different for every session of communication. With symmetric cryptography, the data encryption key sits around until it is used; but using previous protocol, the key is created when it is needed to encrypt communication and destroyed when it is no longer needed. Using public-key cryptography for key distribution solves a very important key-management problem.

There is still one more feature that must be introduced to authentifie from who the first message is received by the server. It can be solved using the digital signature techniques. One of the solution is by providing a private key for each user. A user must encrypt first its key K by its private key, before encrypting it again using the server's public key in thirth step of protocol above. The server try to decrypt it using every public key of its users, and find out the sender when the decryption process is succesfull. The protocol above can be rewritten including the digital signature technics as below :

1. User sends a message to server asking for a connection
2. Server sends its public key P
3. User generate a random key K, encrypts it using its private key V, and encrypts it again using server's public key
   $C = E_P (E_V (K))$
4. User sends the double crypted message to the server
5. Server decrypts client's message using its private key to recover the encrypted key K
   $E_V (K) = D_P (E_P (E_V (K)))$
6. Server than identifie the user by decrypting the encrypted key using each of its user's public key
7. Both of them encrypt their communication using the same key K

By this techniques, the user can be identified. It can not deny its demand because it is recognized by its private key. In the data transfer, the authentication of sender i.e. the server, is assuring by the session key K. The result is that communication between user and database server remains safe and fast.

One eavesdropper can listen all the message exchanged by server and the user, but it is hard to decrypt and to recover the information because it is decrypted by a public key, or session key.

V. CONCLUSION

Several concepts of secured digital communication have been described . According to the caracteristics of data distribution of Seawatch Indonesia, one technics assuring the confidentiality of distributing data and the authentication of message exchanging is proposed. The technics involves hybrid cryptosystem and digital signature algorithm. With the technics, it is save to use the internet network as a communication channel to distribute the data.