Chapter XV
Multimedia Transcoding in Wireless and Mobile Networks: Keyless Self-Encrypting/ Decrypting Scheme for Multimedia Transporting Systems

Shadi R. Masadeh
The Arab Academy for Banking and Financial Sciences, Jordan

Walid K. Salameh
Princess Sumayya University for Technology, Jordan

ABSTRACT

This chapter presents a keyless self-encrypting/decrypting system to be used in various communications systems. In the world of vast communications systems, data flow through various kinds of media, including free air. Thus the information transmitted is free to anyone who can peer it, which means that there should be a guarding mechanism so the information is transmitted securely over the medium from the sender to the intended receiver, who is supposed to get it in the first place and deter the others from getting the information sent. Many encryption systems have been devised for this purpose, but most of them are built around Public Key Infrastructure (PKI) wherein public key cryptography, a public and private key, is created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA). The private key is given only to the requesting party, and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the medium. All of the commonly used encryption systems exchange keys that need to be generated using complex mathematical operations that take noticeable time, which is sometimes done once, and exchanged openly over unsecured medium. We are proposing an expandable keyless self-encrypting/decrypting system, which does not require the use of keys in order o minimize the chances of breaching data exchange security and enhance the data security of everyday communications devices that are otherwise insecured.

INTRODUCTION

The advent of communications systems and computing technology has merged the two technologies in multimedia technology, where data are delivered in multiformat containing both textual, video, and audio data, all in the same frame.

The wide use of the Internet has led to the broader use of information sources and imposed a necessity for information security measures to be used in delivering electronic contents from the sender to the intended receiver.

Since old times and out of pure necessity, people have invented encryption to hide the real meaning of the information they intended to send so the information will be delivered only to the person who is meant to decipher it and understand its contents.

Many schemes were developed throughout the ages, and mathematicians started working on the subject to create a scheme that is unbreakable under any attacks so the information will be secured no matter what the others (code breakers) will do to get the information the encrypted data hides.

Throughout the study of previous encryption systems techniques, people learned about the internals of the different standards used in encryption systems such as DES, Triple DES, RC4, RC5, RC6, and AES (Schneier, 1994).

This chapter presents briefly as excerpts from references the underlying techniques in those encryption systems and their points of weakness and strength.

TERMINOLOGY

Before we discuss encryption and decryption processes, we should get familiar with the terminologies used by cryptographers. Most of the terminology material has been adopted from *Applied Cryptography* by Bruce Schneier.

Sender and Receiver. Suppose a sender wants to send a message to a receiver. Moreover, this sender wants to send the message securely to make sure an eavesdropper cannot read the message.

Messages and Encryption. Any message is regarded as a plain text (sometimes called clear text). The process of disguising a message in such a way as to hide its substance is encryption. An encrypted message is cipher text. The process of turning cipher text back into plain text is decryption. If you want to follow the ISO 7498-2 standard, use the terms "encipher" and "decipher." It seems that some cultures find the terms "encrypt" and "decrypt" offensive, as they may refer to dead bodies.

The art and science of keeping messages secure is cryptography, which is practiced by cryptographers. Cryptanalysts are practitioners of cryptanalysis, the art and science of breaking cipher text; that is, seeing through the disguise. The branch of mathematics encompassing both cryptography and cryptanalysis is cryptology; its practitioners are cryptologists. Modern cryptologists are generally trained in theoretical mathematics—they have to be.

Plain text is denoted by M, for message, or P, for plain text. It can be a stream of bits, a text file, a bitmap, a stream of digitized voice, a digital video image, and so forth. As far as a computer is concerned, M is simply binary data. The plain text can be intended for either transmission or storage; in any case, M