Chapter 1

Introductory Chapter: Recent Advances in Cryptography and Network Security

Pinaki Mitra

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.81283

1. Introduction

In the last few decades, we observed a significant development in the field of computing. Initially, we had mainframe systems. Subsequently, personal computers evolved. The physical size of both processors and storage got reduced. With the advent of new technology, the computing power and storage capability increased. In personal computers, we subsequently observed the amalgamation of parallel processing concepts with the development of multicore chips. But more importantly, the technology that developed rapidly was that of Internet and computer networks [1]. Personal computer interconnected via Internet provides significant computing facility to users. The interconnection is either wired or wireless. The size of these computing devices got further reduced with the advent of mobile computing. The handheld mobile devices provide significant computing facility to the users through wireless interconnection. As the computing technology evolved, there is a significant growth in the volume of communicated data across the network. The increased traffic causes delay in data transmission. So, there is necessity of data compression that can reduce the traffic significantly. Different coding and compression techniques for audio, image, video, text, and graphics data emerged to handle these problems. In audio, we have seen different compression schemes like MP3, AVI, etc. Image compression is achieved using JPEG. In video compression, there had been a series of developments in MPEG techniques. Text compression is achieved through different coding techniques like Huffman [2] encoding or Lempel-Ziv-Welch (LZW) encoding [3, 4].

Another problem that has to be addressed is the security and privacy of the huge amount of communicated information through either wired or wireless transmission media. We observed a significant development in the area of cryptography and network security [5]. The area of cryptography concerns secure communication between sender and receiver that should prevent the eavesdropper to tamper or intercept confidential data. Different encryption and

decryption techniques evolved for this purpose. They are broadly classified into two types: (a) symmetric-key and (b) public-key cryptosystems. In symmetric-key cryptography, the same key is shared between the sender and the receiver. But in public-key cryptography, the sender sends the encrypted data to the receiver using receiver's public key. The receiver decrypts the data using his/her own secret key. There are several cryptographic algorithms for both symmetric- and public-key cryptosystems. **Figure 1** depicts symmetric-key cryptosystem. **Figure 2** depicts public-key cryptosystem. In both figures, the sender is Alice and the receiver is Bob. The unencrypted message M is usually known as plain text. The encrypted message C is called cipher text or in short cipher.

Another important aspect of secure communication is that of nonrepudiation. This is achieved by means of digital signature. In public-key cryptosystem, the sender sends both message and the signature that is the encrypted version of the message with the private/secret key of the sender. **Figure 3**, illustrates the digital signature scheme where the digital signature $S = S_A(M)$ is the message encrypted with the secret key of Alice. The 2-tuple (S, M), i.e., the signature along with the message is transmitted to Bob. At the receiving end, Bob applies the public key of Alice to obtain $M' = P_A(S) = P_A(S_A(M))$ that is supposed be equal to M if the signature is valid. So Bob compares M' and M and accepts if they are equal otherwise Bob rejects. There are several variations of signature schemes and many of them use cryptographic hash functions.

The similar notion of authentication is also used in image data. Several techniques related to that had evolved recently in digital water marking and steganography. Also, there had been a significant development in the field of authentication using biometric data.

With advent of quantum computers, there had been significant development in the area of postquantum cryptography. This is because several computationally difficult problems for classical computing model are susceptible to attacks in quantum computing model. Postquantum cryptographic algorithms had to handle these challenges.

In the area of network security, we had seen different new types of attacks with the advent of mobile computing technology where there are no fixed interconnections among mobile nodes. One frequent type of attack in particular is DDOS or distributed denial of service attack. This attack causes jamming of the network by flooding redundant packets across the network. There are several remedies that had been devised to counter these attacks. Typical information theoretic measures like *precision* and *recall* may be used to evaluate the performance of these remedial techniques with true positives, true negatives, false positives, and false negatives.

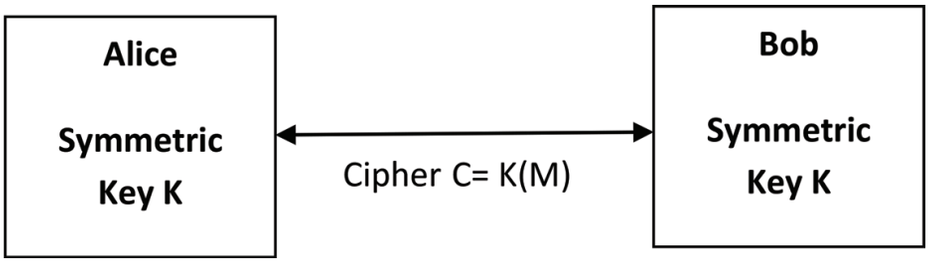

Figure 1. Symmetric-key cryptosystem.

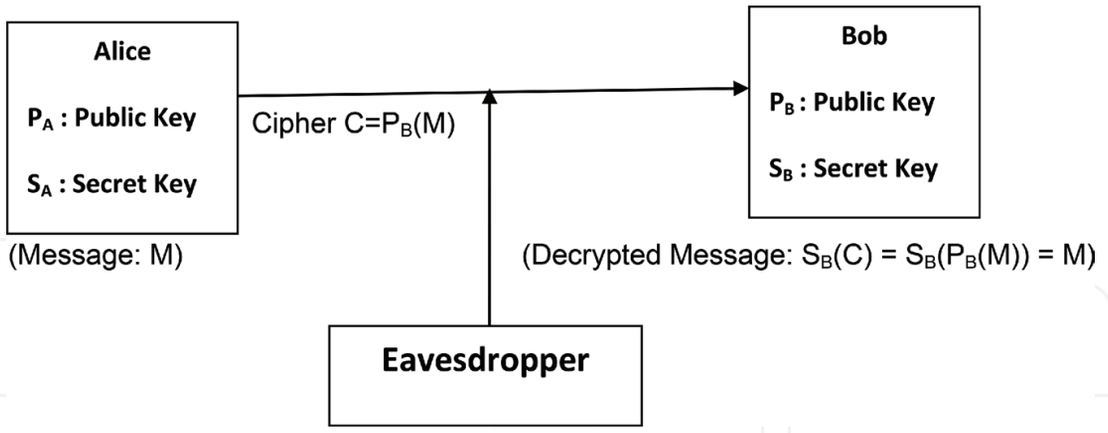

Figure 2. Public-key cryptosystem.

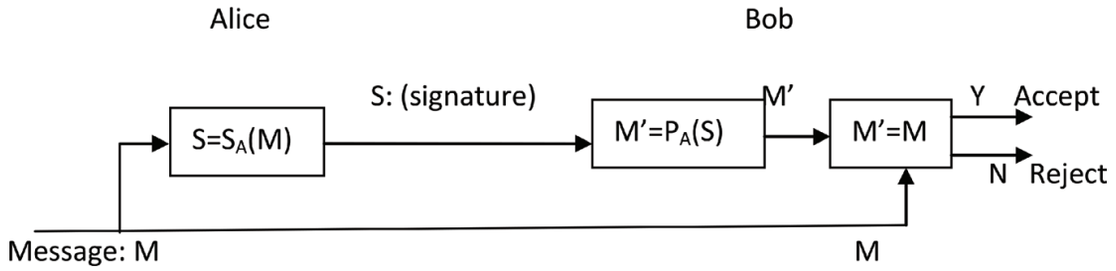

Figure 3. Authentication using digital signature.

Recently, we had seen the advent of IOT or Internet of Things. In a typical house, the household devices, such as television, fridge, microwave, washing machines, smoke detectors, etc. need to communicate with each other to relieve the end user from manual interventions in many real-time processes. Networking protocol TCP/IP was modified with RTP running over UDP for real-time applications. Over and above other issues of concern in this domination is limited computing, storage and energy, i.e., battery power. These devices usually use lightweight encryption/decryption algorithms since they are resource constrained. The major goal here is not to compromise the security and authenticity of the communicated data too much.

2. Conclusion

In the field of computers with the advent of Internet, the topic secure communication gained a significant importance. The theory of cryptography and coding theory evolved to handle many such problems. The emphases of these topics are both on secure communication that uses encryption and decryption schemes as well as on user authentication for the purpose of nonrepudiation. Subsequently, the topics of distributed and cloud computing emerged. Existing results related to cryptography and network security had to be tuned to adapt with these new technologies. More recently with the advancement of mobile technologies and Internet of Things (IOT), these algorithms had to take into consideration of limited resources like battery power, storage, and processor capabilities. This had led to the development of

lightweight cryptography for resource-constrained devices. The topic of network security also had to face many challenges owing to variable interconnection topology instead of a fixed interconnection topology. For this reason the system becomes susceptible to various attacks from eavesdroppers. The book addresses these issues that arise in present day computing environments to overcome these security threats and also presents several possible directions for future research.

Author details

Pinaki Mitra

Address all correspondence to: pinaki@iitg.ac.in

Department of Computer Science and Engineering, IIT Guwahati, Guwahati, India

References

[1] Stallings W. Data and Computer Communications. Upper Saddle River, New Jersey: Pearson Education, Inc.; 2007

[2] Huffman DA. A method for the construction of minimum-redundancy codes. Proceedings of the IRE. 1952;**40**:1098-1101

[3] Welch T. A technique for high-performance data compression. Computer. 1984;**17**(6):8-19

[4] Ziv J, Lempel A. Compression of individual sequences via variable-rate coding. IEEE Transactions on Information Theory. 1978;**24**(5):530-536

[5] Stallings W. Cryptography and Network Security: Principles and Practice. Upper Saddle River, New Jersey: Prentice Hall, Inc.; 2005