Cryptography is the art and science of concealment of information. Without the ability to conceal infor-
mation, the current networked computing environment would not be possible. In the most fundamental
way, cryptography provides a logical barrier to secure information from unauthorized prying eyes. To
understand cryptography, we need to answer four simple yet interrelated questions: What information
do we need to conceal? Why do we need to conceal it and from whom? How can we optimally conceal
it without diminishing its usefulness? And finally, how do we reveal that which was concealed? The
answers to these questions characterize the essence of information and what it represents.

We view the age we live in as the “information age” and our societies as “information societies”. What
mostly characterizes this information age is the pervasiveness of information technologies in our
daily lives. Almost everything we do in the course of our lives creates an electronic footprint resulting
in an explosion in the amount of data that we generate.

Data experts estimate that in 2002 the world generated 5 exabytes of data. This amount of data is
more than all the words ever spoken by human beings. The rate of growth is just as staggering – the
amount of data produced in 2002 was up 68% from just two years earlier (Stuhler, 2010). The size of
the typical business database has grown a hundred-fold during the past five years as a result of internet
commerce, ever-expanding computer systems and mandated recordkeeping by government regula-
tions. The rate of growth in data has not slowed. International Data Corporation (IDC) estimates that
the amount of data generated in 2009 was 1.2 million Petabytes (IDC, 2010). (A Petabyte is a million
gigabytes.) (IDC, 2010). For example, it is estimated that in 2007, the size of world internet’s hard drive
was 161 Billion gigabytes and the volume skyrocketed to 487 Billion gigabytes in 2009 (IDC, 2010).
The research comes from technology consultancy IDC, and their prediction is that the current size of
the internet’s hard drive will double in the next 18 months as more and more net users get interactive.
According to Julian Stuhler (Stuhler, 2010), worldwide data volumes are currently doubling every two
years. Although this seems to be an astonishingly large amount of data, it is paled in compression to what
IDC estimates that amount to be in 2020. IDC estimates that the amount of data generated in 2010 will
be 44 times as much as this year to an incomprehensible amount of 35 Zettabytes, where a Zettabyte
is 1 trillion gigabytes (Stuhler, 2010). IDC reports that by 2020, we will generate 35 trillion gigabytes
of data, enough data to fill a stack of DVDs reaching from the Earth to the moon. To better grasp how
much data this is, consider the following: if one byte of data is the equivalent of this dot (•), the amount
of data produced globally in 2002 would equal the diameter of 4,000 suns. Moreover, that amount prob-
ably doubles every two years (Hardy, 2004). One of the reasons for this astonishingly large growth,
according to a survey by US Department of Commerce, is that an increasing number of Americans are
going online and engaging in several online activities, including online purchases, conducting banking
online, engaging in commerce, and interacting socially. The growth in Internet usage and e-commerce has offered businesses and governmental agencies the opportunity to collect and analyze information in ways never previously imagined. “Enormous amounts of consumer data have long been available through offline sources such as credit card transactions, phone orders, warranty cards, applications and a host of other traditional methods. What the digital revolution has done is increase the efficiency and effectiveness with which such information can be collected and put to use” (Adkinson, Eisenach, & Lenard, 2002). This digital footprint including our digital shadow represents us, as humans, it represents who we are, and how we conduct our lives. It needs to be secured, protected, and managed appropriately. This information presented in the digital form and spread over the world is now very large, and this information requires protection against malicious intrusion, eavesdrops, substitution, falsification, and so on. In addition, information is a critical asset that supports the mission of any organization and protecting this asset is critical to survivability and longevity of the organization. Maintaining and improving information security is critical to the operations, reputation, and ultimately the success and longevity of any organization. Information and the systems that support it are vulnerable to many threats that can inflict serious damage to organizations resulting in significant losses.

Whether we are using credit cards, surfing the Internet or viewing a YouTube video, we are generating data. John Gantz senior vice president of International Data Corporation, states: “About half of your digital footprint is related to your individual actions—taking pictures, sending e-mails, or making digital voice calls. The other half is what we call the ‘digital shadow’—information about you—names in financial records, names on mailing lists, web surfing histories or images taken of you by security cameras in airports or urban centers. For the first time your digital shadow is larger than the digital information you actively create about yourself.” (IDS, 2010) Our digital shadow, the sum of all the digital information generated about us on a daily basis, now exceeds the amount of digital information we actively create ourselves (IDC, 2010). In essence, this digital shadow defines who we are, what we like and what we do. It needs to be protected and secured. Concerns over information security risks can originate from a number of different security threats. They can come from hacking and unauthorized attempts to access private information, fraud, sabotage, theft and other malicious acts or they can originate from more innocuous sources, but no less harmful, such as natural disasters or even user errors. Cryptography provides the most efficient services for defending against these threats and holds great promise as the technology to provide security in cyberspace, especially when security becomes one of top concerns for business worldwide.

Cryptography studies methods of information encryption that prevent an opponent from extracting information contained in the intercepted messages. In this approach the message communicated through the insecure channel is not the original message, but the result of its transformation using a cipher. The opponent must break the cipher, which may prove to be a challenging problem. Cracking of a cipher is the process of extracting relevant information from an encrypted text without knowing the cipher. Besides cracking, the adversary may try to obtain desired information in a number of other ways. The adversary can eavesdrop or monitor transmission of the information by release of message contents or traffic analysis. Another threat that an adversary can create is to try to destroy or modify the information that is being transmitted. This threat requires specific security methods including masquerade and modification of message. A masquerade takes place when one entity pretends to be a different entity. Modification of message simply means that some portion of a legitimate message is altered, or that message is delayed or reordered, to produce an unauthorized effect. Therefore, on the way from one authorized user to another, information must be protected using different tools against different threats.
These tools form an information protecting chain, consisting of links of different kinds, and the adversary, of course, will search for the weakest link in this chain in order to obtain least possible cost. This means that when developing a security strategy, the authorized users must also take into account that it makes no sense to establish a strong link if there are much weaker ones.

Cryptography provides a set of security services to ensure adequate security of the systems or of data transfer to counter the above threats. The services include authentication, data confidentiality, data integrity and non-repudiation (Stallings, 2006, p17). Entity authentication provides confidence in the identity of the entities connected. Data origin authentication provides assurance that the source of data is as claimed in an insecure transmission. Data integrity assures that data received are exactly as sent by an authorized entity. Non-repudiation provides protection against denial by one of the entities involved in a communication. Security services can be mapped to one of security mechanisms whose implementation relies on cryptography: enciphering, digital signature, data integrity, authentication exchange, and notarization. Enciphering is the use mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys. Digital signature is to append data or to cryptographically transform data, which allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery. Data integrity is to ensure that a data unit or stream is not modified by unauthorized adversaries. Notarization is to use a trusted third party to assure certain properties of a data exchange.

Nowadays cryptographic algorithms have already been applied to some cryptographic means like encrypting electronic mails or smart bank cards, and so on. Naturally, the main question that the user asks is whether a given cryptographic tool provides sufficient defense. Whom are we protecting from? What are the capabilities of our opponents? What goals do they pursue? How to measure the level of security? The list of these questions can be extended. The reality is that cryptography has done no more than creating an illusion of a secure system for the users. The security of a system is decided by the weakest link and the real-world constraints make the cryptography much less effective than they are in pure mathematical world. The cryptography in real-world networks and systems has been less effective than cryptography as a mathematical science because of engineering discipline that converts the mathematical promise of cryptographic security into a reality of security. Building real-world cryptographic systems is different from the abstract theories of cryptography with only pure mathematics. Designers and implementers face real-world constraints which are experienced by most cryptographic systems. In order to achieve real-world security goals, cryptographic techniques should be applied in a real-world setting in order to build and engineer a secure cryptographic system. Applied cryptography bridges the gap between cryptographic theory and real-world cryptographic applications. Applied cryptography gives concrete advice about how to design, implement and evaluate cryptographic system within real-world settings.

This book gives guidelines to cryptographic systems with consideration of real-world constraints and opponents. Different systems have different constraints and opponents such as computation constraints, especially those in emerging areas. The constraints and opponents are analyzed first during requirements analysis, and then the cryptographic algorithms and services are selected to achieve the objective of cryptographic system. The system is evaluated against the requirements, constraints and possible threats from opponents. The book discusses applied cryptography as an engineering discipline to meet specific requirements in real-world applications. This book strives to bridge the gap between cryptographic theory and real-world cryptographic applications. This book also delves into the specific security requirements and opponents in various emerging application areas and discusses the procedure about engineering cryptography into system design and implementation. For example, wireless sensor
networks have energy and computation as cryptographic constraints, entity authentication requires zero knowledge, electronic commerce requires fair electronic exchange besides confidentiality, authentication, and integrity. Our main goal is to engineer cryptography into a real-world secure system and to bridge cryptographic algorithms and techniques with real-world constraints of a specific area. This book introduces how to build a secure system in real settings, which is the essence of applied cryptography in information security and privacy.

SECTION 1: CRYPTOGRAPHY IN NETWORKING AND CYBER SPACE

When communication and transaction take place in a digital form, the security of transaction in cyber space have become of critical importance. Cryptography is one of the traditional and effective to fight off massive invasion of individual privacy and privacy and security, guarantee data integrity and confidentiality, and to bring trust in computer networking and cyber space. Cryptography has become the main tool for providing the needed digital security in the modern digital communication medium that far exceeds the kind of security that was offered by any medium before. It ensures confidentiality, integrity, authentication, authorization, and non-repudiation in all data exchanges in cyber space.

The first chapter in Section 1 focuses on cryptography in network security. “Network Security” is authored by Ramakrishna Thurimella and Leemon C. Baird III. The authors examine three pillars of security—confidentiality, integrity, and availability—in the context of networks. Each is explained with known practical attacks and possible defenses against them, demonstrating that strong mathematical techniques are necessary but not sufficient to build practical systems that are secure. They illustrate how adversaries commonly side-step cryptographic protections. In addition, they contend that effective key management techniques, along with privacy concerns must be taken into account during the design of any secure online system. The chapter is concluded with a discussion of open problems for which fundamentally new methods are needed.

The focus of the second chapter in this section, “Cryptography-Based Authentication for Protecting Cyber Systems” authored by Xunhua Wang and Hua Lin, discusses authentication technology in protecting cyber systems. Entity authentication is a fundamental building block for system security and has been widely used to protect cyber systems. This chapter studies the roles of cryptography in the three entity authentication categories: knowledge-based authentication, token-based authentication, and biometric authentication. The roles of cryptography in the following areas are covered: the generation of password verification data, in password-based challenge/response authentication protocol, and in password-authenticated key exchange protocols; both symmetric key-based and private key-based token authentications; and cryptographic fuzzy extractors, which can be used to enhance the security and privacy of biometric authentication. This systematic study of the roles of cryptography in entity authentication will deepen understanding of both cryptography and entity authentication and can help us better protect cyber systems.

SECTION 2: CRYPTOGRAPHY IN E-MAIL AND WEB SERVICES

E-mail and Web services are two major techniques for people to exchange and share information remotely over the Internet. E-mail services are the method of sending and receiving electronic messages over
communication networks. Web services on the other hand provide a channel of accessing interlinked hypermedia via the World Wide Web. As these two methods of network communications turn into the most popular services over the Internet, applied cryptography and secure authentication protocols become indispensable in securing confidential data over public networks.

The first chapter in Section 2 is titled “E-Mail, Web Service and Cryptography”, and is authored by Professor Wasim A Al-Hamdani. This chapter introduces E-mail structure and organization, web service types, their organization and cryptography algorithms which integrated in the E-mail and web services to provide high level of security. The main issue in this chapter is to build the general foundation through definitions, history, cryptography algorithms symmetric and asymmetric, hash algorithms, digital signature, suite B and general principle to introduce the use of cryptography in the E-mail and web service.

The second chapter in Section 2 is titled “Cryptography in E-Mail and Web Services”, and is authored by Professor Wasim A Al-Hamdani. This chapter presents client and Web-based e-mail, next generation e-mail and secure e-mail, followed by cryptography in web service and the last part is the future of web service security. The chapter starts with the integration of cryptography with e-mail client and web base then the integration of cryptography and web service is presented. At the end of the chapter, they present their view for the cryptography integration with the second generation of e-mail and web service.

The third chapter in Section 2 is titled, “Applied Cryptography in E-Mail Services and Web Services” is coauthored by Professors Lei Chen, Wen-Chen Hu, Ming Yang, and Lei Zhang. This chapter first reviews a number of cryptographic ciphers widely used in secure communication protocols. We then discuss and compare the popular trust system Web of Trust, the certificate standard X.509, and the standard for public key systems Public Key Infrastructure (PKI). Two secure e-mail standards, OpenPGP and S/MIME, are examined and compared. The de facto standard cryptographic protocol for e-commerce, Secure Socket Layer (SSL) / Transport Layer Security (TLS), and XML Security Standards for secure web services are also discussed.

SECTION 3: CRYPTOGRAPHY IN WIRELESS COMMUNICATION

The first research chapter in Section 3 deals with a very timely issue of how to secure a wireless sensor network (WSN), which employs a large number of wireless sensors to collectively monitor and disseminate information about an area of interest and is independent from fixed infrastructure. The WSN finds its application in military surveillance, habitat and weather monitoring, and emergency rescue operations. The network is usually deployed in a hostile unattended environment which is vulnerable to various attacks. Challenges faced by enforcing security in WSN lies in energy constraints in tiny sensors and how to implement security in two major techniques in WSN: data aggregation and passive participation. This chapter, titled “Applied Cryptography in Wireless Sensor Networks” is authored by Dulal C. Kar and Hung Ngo. This chapter summarizes, discusses, and evaluates recent symmetric key based results reported in literature on sensor network security protocols such as for key establishment, random key pre-distribution, data confidentiality, data integrity, and broadcast authentication as well as expose limitations and issues related to those solutions for WSNs. They also present significant advancement in public key cryptography for WSNs with promising results from elliptic curve cryptography and identity based encryption as well as their limitations for WSNs.

The second chapter in this section is on “Applied Cryptography in Infrastructure-Free Wireless Networks” authored by Lei Zhang, Danfeng Yao, and Chih-Cheng Chang. This chapter presents the technical
challenges and solutions in securing wireless networks, in particular infrastructure-less wireless networks such as mobile ad hoc networks and wireless sensor networks. Communications in infrastructure-less wireless networks are challenging, as there are no trusted base stations to coordinate the activities of mobile hosts. Applied cryptographic tools, in particular threshold cryptography, play an important role in the trust establishment, message security, and key management in such networks. This chapter also describes several technical approaches that integrate applied cryptography techniques into mobile ad hoc networks and wireless sensor networks.

SECTION 4: CRYPTOGRAPHY IN ELECTRONIC COMMERCE

Electronic commerce has grown into a vital segment of the economy of many nations. It is a global phenomenon providing markets and commercialization opportunities world-wide with a significantly reduced barrier to entry as compared to global marketing in the 20th century. Providing protocols to secure such commerce is critical and continues to be an area for both scientific and engineering study. Falsification, fraud, identity theft, and disinformation campaigns or other attacks could damage the credibility and value of electronic commerce if left unchecked. Consequently, cryptographic methods have emerged to combat any such efforts, be they the occasional random attempt at theft or highly organized criminal or political activities.

The first chapter in Section 4, “Applied Cryptography in Electronic Commerce” is authored by Sławomir Grzonkowski, Brian D. Ensor, and Bill McDaniel. This chapter covers the use of cryptographic methods and emerging standards in this area to provide the necessary protection. That protection, as is common for web-based protocols, evolves over time to deal with more and more sophisticated attacks. At the same time, the provision of security in a manner convenient enough to not deter electronic commerce has driven research efforts to find easier to use and simpler protocols to implement even as the strength of the cryptographic methods has increased. This chapter also introduces current standards, looking at several facets of the secure commercialization problem from authentication to intrusion detection and identity and reputation management. Vulnerabilities are discussed as well as capabilities.

Exchanging in a fair manner is important in electronic commerce. This means both parties obtain what they expect or they obtain nothing at all. The second chapter, “An Electronic Contract Signing Protocol Using Fingerprint Biometrics” by Harkeerat Bedi, Li Yang, and Joseph Kizza investigates vulnerabilities and attacks in existing fair electronic exchange protocols and provide a solution for dispute resolution and countering replay attacks. Involvement of fingerprint biometrics makes authentication stronger and password management easier. The chapter demonstrates how to use cryptography and biometrics to realize confidentiality, integrity, non-repudiation and fairness in electronic commerce.

SECTION 5: CRYPTOGRAPHY IN EMERGING AREAS

We live in a pervasive computing environment formed by devices such as computers, printers, iPods, smartcards, RFID tags, etc. Pervasive computing faces two challenges: dynamic computing environment and unattended devices. Service discovery can help to solve above challenges and simplify communica-
tion among various electronic devices. In the meanwhile, service discovery introduces new security and privacy challenges. The first chapter in Section 5, “Secure and Private Service Discovery in Pervasive Computing Environments” by Feng Zhu and Wei Zhu, discusses how to use a progressive and probabilistic model to protect privacy of both users and service providers. A novel exposure negotiation is proposed to facilitate the communication when two parties expect the other one to expose information first. Users and service providers expose identity, service request and service information progressively in multiple rounds. In each round few bits of information are exchanged. If there is a mismatch at any point, the user or service provider can quit the service discovery process. Because both parties only exchange partial information in multiple rounds, privacy exposure is minimized.

Multimedia data need to be transmitted in a secure manner under certain scenario. However, data encryption standard such as DES, RAS, are not efficient in the encryption of multimedia content due to large volume. The second chapter in this section, “Multimedia Information Security: Cryptography and Steganography”, by Ming Yang, Monica Trifas, Nikolaos Bourbakis, and Lei Chen, attempts to address this issue. The chapter discusses how to encrypt image/video by encrypting only the key parameters in stead of the whole image/video as a bit stream. The chapter also covers how to utilize information hiding to enhance security level of data encryption methodologies, which conceals not only the content of the secret message but also existence of the message. A joint cryptograph-steganography methodology, which combines both encryption and information hiding techniques to ensure information security and privacy in medical images, is also presented.

This third chapter in this section, “Secure Electronic Voting with Cryptography” authored by Xunhua Wang, Ralph Grove, and M. Hossain Heydari discusses computer and network-based voting technologies which have been gradually adopted for various elections. This chapter especially concerns serious security challenges face by computer voting due to the fragile nature of electronic ballots and voting software. This chapter studies the security of computer voting and focuses on a cryptographic solution based on mix-nets. Like traditional voting systems, mix-net-based computer voting provides voter privacy and prevents vote selling/buying and vote coercion. Unlike traditional voting systems, mix-net-based computer voting has several additional advantages: 1) it offers vote verifiability, allowing individual voters to directly verify whether their votes have been counted and counted correctly; 2) it allows voters to check the behavior of potentially malicious computer voting machines and thus does not require voters to blindly trust computer voting machines. Building blocks for the mix-net-based computer voting scheme, including semantically secure encryption, threshold decryption, mix-net, and robust mix-net are given in this chapter.

The fourth chapter “Biometric Security in the E-World” authored by Mayank Vatsa and Kunal Sharma, and A.J. Singh discusses biometrics as a novel authentication and access control supplement to cryptography.

Hamid R. Nemati, PhD.
The University of North Carolina at Greensboro

Li Yang, PhD.
The University of Tennessee at Chattanooga
REFERENCES


