

Review of  
Cryptography: Theory and Practice, Second Edition  
Author of Book: Douglas R. Stinson  
Publisher: CRC Press (339 pages)

William M. Springer II( wmspringer@acm.org)<sup>§</sup>

November 5, 2003

## 1 Introduction

For thousands of years, men have used codes and ciphers to communicate in secret. Historically, the security of a cryptosystem was based in secrecy: the enemy was unaware of how messages were being encoded, and if there were intercepted, would have no idea how to decrypt them. In modern times, messages are often encrypted on the assumption that the enemy knows everything about the cryptosystem, with the exception of the secret key used to encrypt the message. As a result, modern cryptosystems are often mathematically complex, relying on functions that are difficult to break even when massive computing power is brought to bear. Mathematically defined, a cipher is a function which takes as input a plaintext message  $x$  and a key  $k$ , and returns an encrypted message  $y$ . A cryptosystem is often defined as a five-tuple  $(P, C, K, E, D)$  where  $P$  is the set of all possible plaintexts,  $C$  is the set of all possible ciphertexts,  $K$  is the keyspace, or the set of all possible keys, and  $E$  and  $D$  are encryption/decryption functions.  $E$  and  $D$  are chosen such that for every key  $k$ ,  $E_k$  maps  $P$  onto  $C$ ,  $D_k$  maps  $C$  onto  $P$ , and  $D_k(E_k(x)) = x$  for every plaintext element  $x$  in  $P$ . These functions can be anything from simple substitution (replace every  $A$  with  $D$ , for example) to complex mathematical functions.

## 2 Chapter 1: Classical Cryptography

No introduction to cryptography would be complete without mentioning some of the classical ciphers, such as the simple Caesar Cipher, which is a simple shift cipher purportedly used by Julius Caesar. For  $P = C = K = Z_{26}$ , (that is, the plaintext, ciphertext, and keyspace are all integers mod 26, where  $A = 0$ ,  $B = 1$ , etc) we define  $E_k(x) = (x+k) \pmod{26}$  and  $D_k(y) = (y-k) \pmod{26}$ . Other monoalphabetic ciphers covered in this chapter include the Substitution Cipher (where each letter is represented by another letter; this is known as a permutation cipher) and the Affine Cipher (in which the encryption functions are restricted to the form  $e(x) = (ax + b) \pmod{26}$ ). Polyalphabetic ciphers include the Vigenere cipher, which is a shift cipher that uses a different

---

<sup>§</sup>©William Springer 2003

shift for each letter (for example, a Vigenere Cipher with key “cryptography” would encrypt a message as  $(x_1 + 2, x_2 + 17, \dots)$  and the Hill Cipher, which uses matrix multiplication. This chapter also introduces the reader to Alice and Bob (residents of every cryptography text) and to basic cryptanalysis, including ciphertext only, known plaintext, chosen plaintext, and chosen ciphertext attacks. This part of the chapter focuses on frequency analysis, in which the known frequencies of letters and digrams in common English sentences are compared with encrypted letters and digrams in the ciphertext, and the Kasiski text, which is used to determine the key length for polyalphabetic ciphers.

### 3 Chapter 2: Shannon’s Theory

In cryptography, there are three types of security: computational security, which means that the best algorithm for breaking the cryptosystem requires a very large number of operations; provable security, which means that breaking the cryptosystem is at least as hard as solving some other difficult problem, and unconditional security, where the cryptosystem can never be broken even with infinite computational resources.

Proving the security of a cryptosystem involves basic probability theory; for example, if a cryptosystem is unconditionally secure, then the probability that a message is  $x$ , given the encrypted message  $y$ , is the same as the probability that the message is  $x$ ; that is, knowing  $y$  gives you no information about the original message. Shannon gave cryptography the tool of entropy, which in this context is a measure of information or uncertainty. The example used here is the flip of a fair coin; the coin can land either heads or tails with equal probability. As we can encode heads with a 1 and tails with a 0, the information (or entropy) of a coin toss is one bit. Similarly, the entropy of  $n$  coin tosses is  $n$  bits, as we can encode the  $n$  tosses with a string of length  $n$ .

### 4 Chapter 3: Block Ciphers and the Advanced Encryption Standard

Introduced briefly at the end of chapter 2, product ciphers encrypt a message normally, then encrypt it again using a different key or method. The AES cipher, which is now the official standard for encryption, is one such cryptosystem. AES, which accepts keys of length 128, 192, or 256 bits, and breaks the message into blocks of 128 bits, goes through a variable number of rounds depending on the length of the key. If the key is 128 bits, 10 rounds are required, increasing to 12 for 192 bits and 14 for 256 bits. In each round, a variety of operations (mainly row and column shifts) are performed, thoroughly scrambling the original message. A new and widely tested cryptosystem (AES was originally Rijndael, one of 15 AES candidates accepted by the NIST (National Bureau of Standards, now the National Institute of Science and Technology) and went through three years of inspection and testing before being accepted in late 2001), AES is secure against all known attacks, meaning ! that there are no attacks known which are significantly faster than an exhaustive search of the keyspace. This chapter covers the old Data Encryption Standard (DES), AES, Linear Cryptanalysis, and Differential Cryptanalysis.

## 5 Chapter 4: Cryptographic Hash Functions

While encrypting data may keep it from being read, the encryption is no guarantee against the data being altered. Hash functions can be used to create an authentication code, or fingerprint, insuring that the message received is the same as the message that was sent. This chapter covers several algorithms for authorization codes and evaluates their security.

## 6 Chapter 5: The RSA Cryptosystem and Factoring Integers

In most cryptosystems, the decryption function is the same as the encryption function, or is easily derived from it; such a system is called a symmetric-key cryptosystem. In a symmetric-key cryptosystem, the communicating parties share a common key, which must be kept secret; this can lead to problems with key distribution. RSA, invented in 1977 by Rivest, Shamir, and Adleman, is an example of a public-key cryptosystem. Public-key encryption relies on so-called one-way functions, where the encryption function is easy to compute from the decryption function, but not the inverse. One commonly used function is factoring large numbers; given two large primes, it is easy to multiply them together, but difficult to find the original numbers given the product. RSA uses this function; two large primes  $p$  and  $q$  are chosen to be 512-bit primes, making the product a 1024-bit number. This chapter discusses several results from number theory, including the Euclidean Algorithm and the Chinese Remainder Theorem, then discusses the RSA cryptosystem, testing for primes, factoring, and other attacks on RSA.

## 7 Chapter 6: Public-Key Cryptosystems Based on the Discrete Log Problem

As previously mentioned, public key cryptosystems depend on having appropriate one-way mathematical functions; one such is the discrete logarithm problem. The security of these cryptosystems is based on the fact that finding discrete logarithms is generally difficult, while exponentiation is relatively easy. Several cryptosystems built around discrete logarithms are described, including the well-known ElGamal Cryptosystem. This chapter also discusses similar systems based on finite fields and elliptic curves; the end of the chapter covers the security of ElGamal systems and the Diffie-Hellman problems, which are problems related to Diffie-Hellman key agreement protocols.

## 8 Chapter 7: Signature Schemes

In the physical world, documents often require signatures to verify their validity. The same holds true for digital documents, but special problems apply. First, there must be a way to guarantee that the signature is genuine; it must come from the person it purports to belong to. Secondly, the signature must be somehow bound to the document, so that a valid signature cannot be copied onto something entirely different. Finally, there must be a way to prevent reuse; it would hardly do for a digital dollar to be spent multiple times!

Signature schemes are similar to public key encryption, and indeed they work well together. For example, suppose Alice is sending a message to Bob. After writing her message, she computes a signature based on the message (so it cannot be reused for a different message) and encrypts it

using her private key; she then encrypts both the message and the signature using Bob's public key. When Bob receives the message, he decrypts it using his private key, then uses Alice's public key to decrypt her signature and verify that she sent the message.

## 9 Conclusion

I felt that the book was quite readable, although the reader will probably want to be familiar with the terminology of group theory before attempting it. The typos occasionally make a section unclear; the beginning reader will want to correct them using the errata listing at <http://www.cacr.math.uwaterloo.ca/dstinson/CTAP2/errata.html>. My main complaint is the price of the book; for nearly \$80 you get a relatively short book (barely over 300 pages) which leaves out some important topics such as Quantum Cryptography; those subjects are scheduled to appear in a companion volume.