Chapter 10
Basic Cryptography

YORK: Then, York, be still awhile, till time do serve:
Watch thou and wake when others be asleep,
To pry into the secrets of the state;
— *The Second Part of King Henry the Sixth*, I, i, 249–260.

Cryptography is a deep mathematical subject. Because this book focuses on system security, we consider cryptography as a supporting tool. Viewed in this context, the reader needs only a brief overview of the major points of cryptography relevant to that use. This chapter provides such an overview.

Cryptographic protocols provide a cornerstone for secure communication. These protocols are built on ideas presented in this chapter and are discussed at length in later chapters.

10.1 Cryptography

The word *cryptography* comes from two Greek words meaning "secret writing" and is the art and science of concealing meaning. *Cryptanalysis* is the breaking of codes. The basic component of cryptography is a *cryptosystem*.

Definition 10–1. A *cryptosystem* is a 5-tuple $(\mathcal{E}, \mathcal{D}, \mathcal{M}, \mathcal{K}, \mathcal{C})$, where $\mathcal{M}$ is the set of *plaintexts*, $\mathcal{K}$ the set of *keys*, $\mathcal{C}$ is the set of *ciphertexts*, $\mathcal{E} : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{C}$ is the set of *enciphering functions*, and $\mathcal{D} : \mathcal{C} \times \mathcal{K} \rightarrow \mathcal{M}$ is the set of *deciphering functions*.

EXAMPLE: In the latter days of the Roman Republic, Julius Caesar was preparing to invade Italy. His confidential communications with his secret allies in Rome were enciphered using a cipher in which the letters are shifted by 3 (so this type of cipher is called a *shift cipher* or a *Caesar cipher*). For example, the letter "A" becomes "D," "B" becomes "E," and so forth, ending with "Z" becoming "C."

So the word "HELLO" is enciphered as "KHOOR." Informally, this cipher is a cryptosystem with

$$\begin{aligned}\mathcal{M} &= \{\text{all sequences of Roman letters}\}\\ \mathcal{K} &= \{i \mid i \text{ an integer such that } 0 \leq i \leq 25\}\\ \mathcal{E} &= \{E_k \mid k \in \mathcal{K} \text{ and } \forall(m = m_1 \ldots m_n \in \mathcal{M})[E_k(m_i) = (m_i + k) \bmod 26]\}\end{aligned}$$

Representing each letter by its position in the alphabet (with "A" in position 0), "HELLO" is 7 4 11 11 14; if $k = 3$, the ciphertext is 10 7 14 14 17, or "KHOOR."

$$\mathcal{D} = \{D_k \mid k \in \mathcal{K} \text{ and } \forall(c = c_1 \ldots c_n \in \mathcal{C})[D_k(c_i) = (26 + c_l - k) \bmod 26]\}$$

Each D_k simply inverts the corresponding E_k. We also have

$$\mathcal{C} = \mathcal{M}$$

because $\mathcal{E}$ is clearly a set of onto functions.

The primary goal of cryptography is to keep enciphered information secret, thereby countering the threat of disclosure (see Section 1.2). Cryptography can also be used to provide integrity of both data and origin, thereby countering the threats of modification and masquerading. It can also provide nonrepudiation, countering the threat of repudiation of origin. Thus, it is a remarkably powerful mechanism that computer security techniques rely on heavily.

Cryptosystems are based on two types of transformations [1725]. The first, *onfusion*, replaces parts of the plaintext message with other data, to hide the original content. The second, *diffusion*, scrambles the plaintext message so that the original content is spread throughout the message. These increase the difficulty of uncovering the original plaintext message.

10.1.1 Overview of Cryptanalysis

Cryptanalysis is the analysis of cryptosystems in order to decipher the messages. *Kerckhoff's Principle* says that the security of a cryptosystem cannot rely on an adversary's not knowing the algorithms for encryption and decryption [1826]. Thus, standard cryptographic practice is to assume that she knows the algorithms used to encipher and decipher, and the set of possible keys, but not the specific cryptographic key (in other words, she knows $\mathcal{K}$, $\mathcal{D}$, and $\mathcal{E}$).

An adversary may use three types of attacks:

- In a *ciphertext only* attack, the adversary has only the ciphertext. Her goal is to find the corresponding plaintext. If possible, she may try to find the key, too.

- In a *known plaintext* attack, the adversary has the ciphertext and the plaintext that was enciphered. Her goal is to find the key that was used.
- In a *chosen plaintext* attack, the adversary may ask that specific plaintexts be enciphered. She is given the corresponding ciphertexts. Her goal is to find the key that was used.

A good cryptosystem protects against all three.

Attacks use both mathematics and statistics. The mathematical methods examine the assumptions of the problems upon which the security of the ciphers rests. The statistical methods make assumptions about the statistics of the plaintext language and examine the ciphertext to correlate its properties with those assumptions. Those assumptions are collectively called a *model* of the language. Common models of language are 1-gram models (reflecting frequence of individual letters), 2-gram models (reflecting frequencies of pairs of letters), Markov models, and word models.

10.2 Symmetric Cryptosystems

Symmetric cryptosystems (also called *single key* or *secret key* cryptosystems) are cryptosystems that use the same key for encipherment and decipherment. In these systems, for all $c \in \mathcal{C}$ and $k \in \mathcal{K}$, there is a $D_k \in \mathcal{D}$ such that $D_k(E_k(m)) = m$.

EXAMPLE: The shift cipher discussed earlier had a key of 3, so the enciphering function was E_3. To decipher "KHOOR," we used the same key in the decipherment function D_3. Hence, the shift cipher is a symmetric cipher.

There are two basic types of symmetric ciphers: *transposition* ciphers that diffuse the data in the plaintext and *substitution* ciphers that replace the data in the plaintext.

10.2.1 Transposition Ciphers

A *transposition cipher* rearranges the characters in the plaintext to form the ciphertext. The letters are not changed. Thus, each encryption key $k \in \mathcal{K}$ indicates a permutation algorithm. The set of encryption functions $\mathcal{E}$ is simply the set of permutations of m, and the set of decryption functions $\mathcal{D}$ is the set of inverse permutations.

EXAMPLE: The *rail fence cipher* is composed by writing the plaintext in two rows, proceeding down, then across, and reading the ciphertext across, then down. For example, the plaintext "HELLO, WORLD" would be written as

```
HLOOL
ELWRD
```

resulting in the ciphertext "HLOOLELWRD."

Mathematically, the key to a transposition cipher is a permutation function. Because the permutation does not alter the frequency of plaintext characters, a transposition cipher can be detected by comparing character frequencies with a model of the language. If, for example, character frequencies for 1-grams match those of a model of English, but 2-gram frequencies do not match the model, then the text is probably a transposition cipher.

Attacking a transposition cipher requires rearranging the letters of the ciphertext. This process, called *anagramming*, uses tables of *n*-gram frequencies to identify common *n*-grams. The cryptanalyst arranges the letters in such a way that the characters in the ciphertext form some *n*-grams with highest frequency. This process is repeated, using different *n*-grams, until the transposition pattern is found.

EXAMPLE: Consider the ciphertext "HLOOLELWRD." According to Konheim's digram table [1092, p. 19], the digram "HE" occurs with frequency 0.0305 in English. Of the other possible digrams beginning with "H," the frequency of "HO" is the next highest, at 0.0043, and the digrams "HL," "HW," "HR," and "HD" have frequencies of less than 0.0010. Furthermore, the frequency of "WH" is 0.0026, and the digrams "EH," "LH," "OH," "RH," and "DH" occur with frequencies of 0.0002 or less. This suggests that "E" follows "H." We arrange the letters so that each letter in the first block of five letters (from '"H" up to but not including the "E") is adjacent to the corresponding letter in the second block of five letters, as follows:

```
HE
LL
OW
OR
LD
```

Reading the letters across and down produces "HELLOWORLD." Note that the shape of the arrangement is different from that in the previous example. However, the two arrangements are equivalent, leading to the correct solution.

10.2.2 Substitution Ciphers

A *substitution cipher* changes characters in the plaintext to produce the ciphertext.

EXAMPLE: The shift cipher discussed earlier had a key of 3, altering each letter in the plaintext by mapping it into the letter three characters later in the

alphabet (and circling back to the beginning of the alphabet if needed). This is a substitution cipher.

A shift cipher is susceptible to a statistical ciphertext-only attack.

Figure 10–1 presents a character-based, or 1-gram, model of English text; others are 2-gram models (reflecting frequencies of pairs of letters), Markov models, and word models. In what follows, we use the 1-gram model and assume that the characters are chosen independently of one another.

EXAMPLE: Consider the ciphertext "KHOOR ZRUOG." We first compute the frequency of each letter in the ciphertext:

G	0.1	H	0.1	K	0.1	O	0.3	R	0.2	U	0.1
Z	0.1										

We now apply the character-based model. Let $\phi(i)$ be the correlation of the frequency of each letter in the ciphertext with the character frequencies in English (see Figure 10–1). Let $\phi(c)$ be the frequency of character c (expressed as a fraction). The formula for this correlation for this ciphertext (with all arithmetic being mod 26) is

$$\varphi(i) = \sum_{0 \le c \le 25} \phi(c)p(c-i) = 0.1p(6-i) + 0.1p(7-i) + 0.1p(10-i)$$
$$+0.3p(14-i) + 0.2p(17-i) + 0.1p(20-i) + 0.1p(25-i)$$

This correlation should be a maximum when the key k translates the ciphertext into English. Figure 10–2 shows the values of this function for the values of i. Trying the most likely key first, we obtain as plaintext "EBIIL TLOIA" when $i = 6$, "AXEEH PHKEW" when $i = 10$, "HELLO WORLD" when $i = 3$, and "WTAAD LDGAS" when $i = 14$.

The example above emphasizes the statistical nature of this attack. The statistics indicated that the key was most likely 6, when in fact the correct key was 3. So the attacker must test the results. The statistics simply reduce the number of trials in most cases. Only three trials were needed, as opposed to 13 (the expected number of trials if the keys were simply tried in order).

a	0.07984	h	0.06384	n	0.06876	t	0.09058
b	0.01511	i	0.07000	o	0.07691	u	0.02844
c	0.02504	j	0.00131	p	0.01741	v	0.01056
d	0.04260	k	0.00741	q	0.00107	w	0.02304
e	0.12452	l	0.03961	r	0.05912	x	0.00159
f	0.02262	m	0.02629	s	0.06333	y	0.02028
g	0.02013					z	0.00057

Figure 10–1 Table of character frequencies in the English language

i	$\varphi(i)$	i	$\varphi(i)$	i	$\varphi(i)$	i	$\varphi(i)$
0	0.0469	7	0.0461	13	0.0505	19	0.0312
1	0.0393	8	0.0194	14	0.0561	20	0.0287
2	0.0396	9	0.0286	15	0.0215	21	0.0526
3	0.0586	10	0.0631	16	0.0306	22	0.0398
4	0.0259	11	0.0280	17	0.0386	23	0.0338
5	0.0165	12	0.0318	18	0.0317	24	0.0320
6	0.0676					25	0.0443

Figure 10–2 The value of $\varphi(i)$ for $0 \leq i \leq 25$ using the model in Figure 10–1.

EXAMPLE: Using Konheim's model of single-character frequencies [1092, p. 16], the most likely keys (in order) are $i = 6$, $i = 10$, $i = 14$, and $i = 3$. Konheim's frequencies are different than Denning's, and this accounts for the change in the third most probable key.

A variant of the shift cipher, called an *affine cipher*, uses a multiplier in addition to the shift. Exercise 4 examines this cipher.

10.2.2.1 Vigenère Cipher

The shift cipher maps every character into another character in one alphabet. Such a cipher is a *monoalphabetic* cipher. As noted above, it preserves the statistics of the underlying message, which a cryptanalyst can use to decipher the message.

A *polyalphabetic* cipher uses multiple alphabets to generate the ciphertest, thereby obscuring the statistics. The Vigenère cipher is such a cryptosystem. In it, the key is a sequence of letters. The key letters are applied to successive plaintext characters, and when the end of the key is reached, the key starts over. The length of the key is called the *period* of the cipher. Figure 10–3 shows a *tableau*, or table, to implement this cipher efficiently. Because this requires several different key letters, this type of cipher is called *polyalphabetic*.

EXAMPLE: The first line of a limerick is enciphered using the key "BENCH," as follows:

```
Key         B ENCHBENC HBENC HBENCH BENCHBENCH
Plaintext   A LIMERICK PACKS LAUGHS ANATOMICAL
Ciphertext  B PVOLSMPM WBGXU SBYTJZ BRNVVNMPCS
```

For many years, the Vigenère cipher was considered unbreakable. Then a Prussian cavalry officer, Major Kasiski, noticed that repetitions occur when characters of the key appear over the same characters in the ciphertext. The

	A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 10–3 The Vigenère tableau.

number of characters between the repetitions is a multiple of the period. From this observation, he developed an effective attack.

EXAMPLE: Let the message be "THE BOY HAS THE BAG" and let the key be "VIG." Then

Key	VIGVIGVIGVIGVIG
Plaintext	THEBOYHASTHEBAG
Ciphertext	OPKWWECIYOPKWIM

In the ciphertext, the string "OPKW" appears twice. Both are caused by the key sequence "VIGV" enciphering the same ciphertext, "THEB." The ciphertext repetitions are nine characters apart. As Figure 10–4 shows, the lower this value, the less variation in the characters of the ciphertext and, from our models of English, the longer the period of the cipher.