A Note on Cryptography

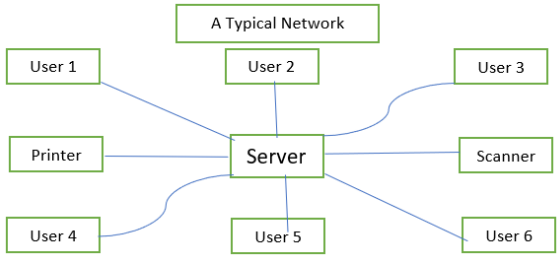
Dr. Madhusudhan H. S.
Assistant Professor of Mathematics, Government First Grade College, Bannur, Mysore

Abstract: ***In this paper we discuss basics of cryptography and their uses. We discuss one important cryptosystem called RSA cryptosystem that is based on the difficulty of factoring a large integer***

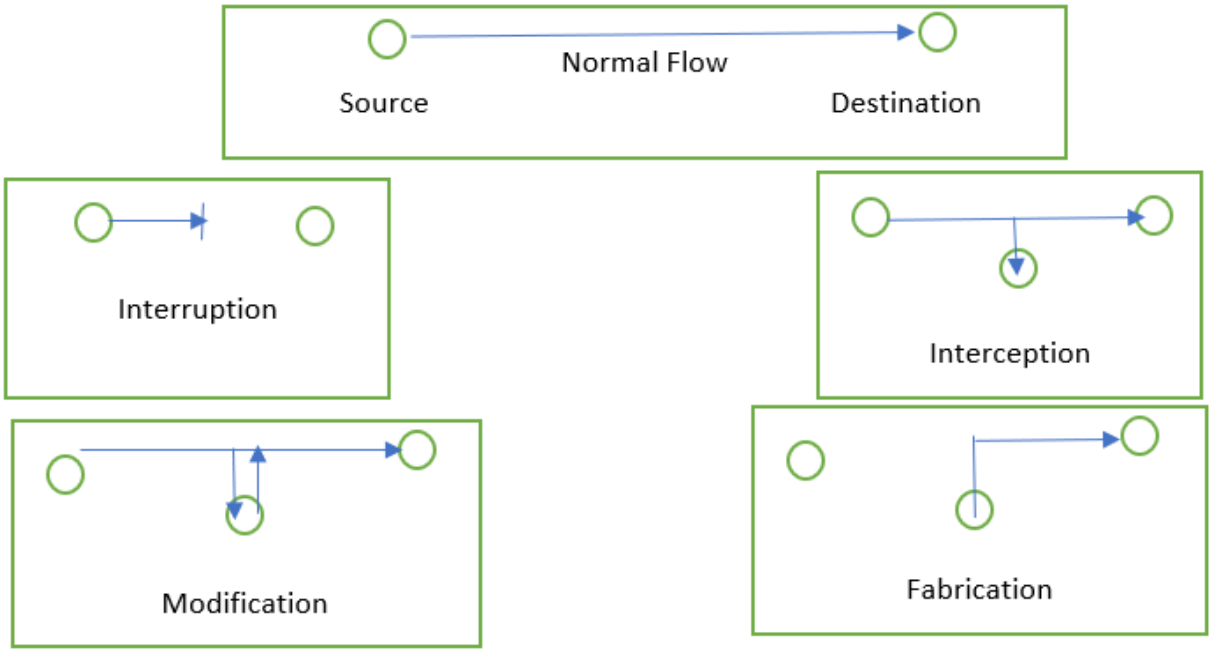
Keywords: Computer, communication, cryptosystem, cryptanalysis, factorization, plaintext, ciphertext, symmetric and asymmetric keys, enciphering and deciphering keys, encryption and decryption, RSA cryptosystem.

INTRODUCTION

The proliferation of computers and communication systems in the 1960s brought with it a demand from the private sector for means to protect information in digital form and to provide security services. In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed no time at which security does not matter. Two trends have come together to make the topic of vital interest. First, the explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This, in turn, has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Second, the disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security.



Security attacks: The following figure shows 4 types of typical security attacks.



- Interruption: An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, such as hard disk, the cutting of a communication line etc.,
- Interception: An unauthorized party gains access to an asset. This is an attack on confidentiality. Examples include wiretapping to capture data in a network, and the illicit copying of files or programs
- Modification: An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. Examples include changing values in a data file, altering a program so that it performs differently etc.,
- Fabrication: An unauthorized party inserts counterfeit objects in the system. This is an attack on authenticity. Examples include the insertion of spurious message in a network or the addition of records to a file.

CRYPTOGRAPHY

Definition 1: Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called the *plaintext* and the disguised message is called the *ciphertext*. The plaintext and ciphertext are written in some alphabet (usually, but not always, they are written in the same alphabet) consisting of a certain number *N* of *letters*. The term "letter" (or "character") can refer not only to the familiar A-Z, but also to numerals, blank, punctuation marks, or any other symbols that we allow ourselves to use when writing the messages. The process of converting a plaintext to a ciphertext is called *enciphering* or *encryption*, and the reverse process is called *deciphering* or *decryption*.

The plaintext and ciphertext are broken up into *message units.* A message unit might be a single letter, a pair of letters (digraph), a triple of letters (*trigraph*), or a block of 50 letters. An *enciphering transformation* is a function that takes any plaintext messages unit and gives us a ciphertext message unit. In other words, it is a map *f* from the set *P* of all possible plaintext message units to the set *C* of all possible ciphertext message units.We shall always assume that *f* is a 1-to-1 correspondence. That is, given a ciphertext message unit, there is one and only one plaintext message unit for which it is the encryption. The *deciphering transformation* is the map f^{-1} which goes back and recovers the plaintext from the ciphertext. We can represent the situation schematically by the diagram

$$P \xrightarrow{f} C \xrightarrow{f^{-1}} P.$$

Any such set-up is called a *cryptosystem.*

The first step in inventing a cryptosystem is to "label" all possible plaintext message units and all possible ciphertext message units by means of mathematical objects from which functions can be easily constructed. These objects are often simply the integers in some range. For example, if our plaintext and ciphertext message units are single letters from the 26- letter alphabet A-Z, then we can label the letters using the integers 0, 1, 2,…, 25, which we call their "numerical equivalents". Thus, in place of A we write 0, in place of S we write 18, in place of X we write 23, and so on. As another example, if our message units are digraphs in the 27- letter alphabet consisting of A-Z and a blank, we might first let the blank have numerical equivalent 26 (one beyond Z), and then label the digraph whose two letters correspond to $x, y \in \{0,1, \ldots.,728\}$.

Thus, we view the individual letters as digits to the base 27 and we view the digraph as a 2-digit integer to that base. For example, the digraph "NO" corresponds to the integer 27. 13 + 14 = 365. Analogously, if we were using trigraphs as our message units, we could label them by integers $729x+27y+z \in \{0,1, \ldots.,19682\}$. In general, we can label blocks of *k* letters in an *N*-letter alphabet by integers between 0 and $N^k - 1$ by regarding each such block as a *k*-digit integer to the base *N.*

Examples. Let us start with the case when we take a message unit (of plaintext or of ciphertext) to be a single letter in an *N*-letter alphabet labeled by the integers 0, 1, 2,…, $N - 1$. Then, by definition, an enciphering transformation is a rearrangement of those *N* integers.

To facilitate rapid enciphering and deciphering, it is convenient to have a relatively simple rule for performing such a rearrangement. One way is to think of the set of integers $\{0, 1, 2, \cdots, N-1\}$ as *Z/NZ*, and make use of the operations of addition and multiplication modulo *N.*

Suppose we are using the 26–letters alphabet A – Z with numerical equivalents 0 – 25. Let the letter $P \in$

$\{0, 1, \cdots, 25\}$, stand for a plaintext message unit. Define a function *f* from the set $\{0, 1, \cdots, 25\}$ to itself by the rule

$$f(P) = \begin{cases} P + 3, & if\ x < 23, \\ P - 23, & if\ x \geq 23. \end{cases}$$

In other words, *f* simply adds 3 modulo 26: $f(P) \equiv P + 3\ mod\ 26$. The definition using modular arithmetic is easier to write down and work with. Thus, with this system, to encipher the word "YES" we first convert to numbers: 24 4 18, then add 3 modulo 26: 1 7 21, then translate back to letters: "BHV." To decipher a message, one subtracts 3 modulo 26. For example, the ciphertext "ZKB" yields the plaintext, "WHY." This cryptosystem was apparently used in ancient Rome by Julius Caesar, who supposedly invented it himself.

The above example can be generalized as follows. Suppose we are using an *N*-letter alphabet with numerical equivalent 0, 1,⋯ , $N - 1$. Let *b* be a fixed integer. By a *shift* transformation we mean the enciphering function *f* defined by the rule $C = f(P) \equiv P + b\ mod\ N$. Julius Caesar's cryptosystem defined by the rule $C = f(P) \equiv P + b\ mod\ N$. Julius Caesar's cryptosystem was the case $N = 26$, $b = 3$. To decipher a ciphertext message unit $C \in \{0, 1, \cdots, N - 1\}$, we simply compute $P = f^{-1}(C) \equiv C - b\ mod\ N$. Here *b* is the encryption key and is usually deonated by *e* and $N - b$ is the decryption key and is denoted by *d*.

Definition 2: A cryptosystem is called a *block cipher* if its plaintext space and its ciphertext space are the set all possible message units of a fixed length *n*. The *block length n* is a positive integer. A simple example of a block cipher is the Caesar cipher. It has block length 1. In general, block ciphers with block length 1 are called *substitution ciphers.*

SYMMETRIC AND ASYMMETRIC CRYPTOSYSTEMS

We briefly explain the difference between symmetric and asymmetric cryptosystems. If Veena wants to send an encrypted message to Varun, then she uses an encryption key *e* and Varun uses the corresponding decryption key to recover the plaintext. If in a cryptosystem the encryption key *e* is always equal to the decryption key *d*, or if *d* can be easily computed from *e*, then the cryptosystem is called *symmetric.* If Veena and Varun use a symmetric cryptosystem, they must exchange the secret key *e* before they start their communication. Secure key exchange is a major problem. The key *e* must be kept secret since anybody who knows *e* can determine the corresponding decryption key *d.* The Caesar cipher is an example of a symmetric cryptosystem. The keys for encryption and decryption are equal in this system.

In *asymmetric cryptosystems*, the keys *d* and *e* are distinct, and the computation of *d* from *e* is infeasible. In such systems, the encryption key can be made public. If Varun wants to receive encrypted messages, he publishes an encryption key *e* and keeps the corresponding decryption key *d* secret. Anybody can use *e* to encrypt messages for Varun. Therefore, *e* is called the *public key.* But only Varun can decrypt the messages, so *d* is called the *private key.* Asymmetric cryptosystems are also called *public-key cryptosystems.*

Definition 3: An encryption scheme is said to be *breakable* if a third party, without prior knowledge of the key pair (*e*, *d*), can systematically recover plaintext from corresponding ciphertext within some appropriate time frame.

Cryptanalysis: Cryptanalysis deals with the attacks on cryptosystems. In this section, we classify those attacks.

To make attacks on cryptosystems more difficult, one can keep the cryptosystem secret. However, it is not clear how much security is really gained in this way because an attacker has many ways of finding out which cryptosystem is used. He can try to tell from intercepted ciphertexts which system is used. He can also try to get information from people who have information about the encryption scheme in use. Modern cryptanalysis therefore assumes that an attacker knows which cryptosystern is used. Only the (private) keys and the plaintexts are assumed to be secret. The attacker tries to recover plaintexts from ciphertexts or even tries to find out which keys are used. There are the following types of attacks:

- *Ciphertext-only attack.* The attacker knows ciphertexts and tries to recover the corresponding plaintexts or the key.
- *Known-plaintext attack*: The attacker knows a plaintext and the corresponding ciphertext or several such pairs. He tries to find the key used or to decrypt other ciphertexts.

- *Chosen-plaintext attack*:. The attacker is able to encrypt plaintexts but does not know the key. He tries to find the key used or to decrypt other ciphertexts.
- *Adaptive chosen-plaintext attack*: The attacker is able to encrypt plaintexts. He is able to choose new plaintexts as a function of the ciphertexts obtained but does not know the key. He tries to find the key used or to decrypt other ciphertexts.
- *Chosen-ciphertext attack*: The attacker can decrypt but does not know the key. He tries to find the key.

There are many ways to mount these attacks. A simple ciphertext-only attack consists of decrypting the ciphertext with all possible keys. This attack is called *exhaustive search.* The correct plaintext is among the few sensible texts that the attacker obtains. Given the speed of modern computers, this attack is successful for many cryptosystems. It works, for example, for the DES (Data Encryption Standard) system, which until recently was the U.S. encryption standard. A known-plaintext attack may use the statistical properties of the plaintext language. For example, if we apply the Caesar cipher, then for a fixed key any plaintext symbol is replaced by the same ciphertext symbol. The most frequent plaintext symbol is encrypted to the most frequent ciphertext symbol. Since we know the most frequent symbol of the plaintext language, we have a good guess how to decrypt the most frequent ciphertext symbol. Analogously, the frequency of other individual symbols, of pairs, triplets, etc., in the plaintext may be reflected in the ciphertext and can be used to decrypt the ciphertext or to recover the key.

Let us cryptanalyse the the Caesar cipher. The most frequently occurring letter in the ciphertext correspond to those in the plaintext. For example, E is the most frequently occurring letter in an arbitrary text, occurring about 12.5% of the time; the next three letters are T, A, and O, occurring about 9%, 8%, and 8% of the time, respectively.

Consider the ciphertext message:

SLABZ ULCLY ULNVA PHALV BAVMM LHYIB ASLAB ZULCL YMLHY AVULN VAPHAL

The most frequently occurring letter in the ciphertext is L, so our best guess is that it must correspond to the plaintext letter E. Since their ordinal numbers are 11 and 4, this implies $11 \equiv 4 + k(mod\ 26)$; that is, k = 7. Then $C \equiv 4 + k(mod\ 26)$. Using this congruence, we can determine the ordinal number of each letter in the plaintext. After obtaining the ordinal number of each plaintext letter, the plaintext message reads as

LET US NEVER NEGOTIATE OUT OF FEAR BUT LET US NEVER FEAR TO NEGOTIATE

Affine Ciphers: Shift ciphers belong to a large family of affine ciphers defined by the formula

$$C \equiv aP + k(mod\ 26)$$

where a is a positive integer ≤ 25 and $(a, 26) = 1$. Since (a, 26) = 1, inverse of a exists and so

$P \equiv a^{-1}(C - k)(mod\ 26)$.

Since $(a, 26) = 1$, there are $\phi(26) = 12$ choices for a, so there are $12 \cdot 26 = 312$ affine ciphers. One of them is the $C \equiv P(mod\ 26)$ identity transformation corresponding to $a = 1$ and $k = 0$.

When $a = 5$ and $k = 11$, $C \equiv 5P + 11(mod\ 26)$. If $P = 8$, then $\equiv 5 \cdot 8 + 11 \equiv (mod\ 26)$, so under the affine cipher $C \equiv 5P + 11(mod\ 26)$, the letter I is transformed into Z and letter Q into N. Table shows the plaintext letters and the corresponding ciphertext letters created by this affine cipher, which shifts A to L and in which each successive letter is paired with every fifth letter.

Plaintext letter	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
	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
iphertext letter	11	16	21	00	05	10	15	20	25	04	09	14	19	24	03	08	13	18	23	02	07	12	17	22	01	06
	L	Q	V	A	F	K	P	U	Z	E	J	O	T	Y	D	I	N	S	X	C	H	M	R	W	B	G

Hence, under the above affine transformation, the plaintext message THE MOON IS MADE OF CREAM CHEESE will be transformed into THEMO ONISM ADEOF CREAM CHEES E (grouping into 5 letters).

To decipher the message, we use the congruence $P \equiv 5^{-1}(C - 11) \equiv 21(C - 11) \equiv 21C + 3(mod\ 26)$.

Let us cryptanalyze the ciphertext BYTUH NCGKN DUBIH UVNYX HUTYP QNGYV IVROH GSU that was generated by an affine cipher.

First make the frequency analysis of the letters in the ciphertext. According to it U occurs 5 times, H, N, and Y occurs 4 times each. It is reasonable to assume that the letter U corresponds to the letter E in the plaintext message, that is, $20 \equiv 4a + k(mod\ 26)$. If we assume H corresponds to T, then $7 \equiv 19a + k(mod\ 26)$. Solving this linear system, we get $a \equiv 13(mod\ 26)$ and $k \equiv 20(mod\ 26)$, so $C \equiv 13P + 20(mod\ 26)$. But (13, 26) ≠ 1, so this is not a valid cipher. Thus, our guess that H corresponds to T was not a valid one.

So let us assume that N corresponds to T. This yields the linear system $20 \equiv 4a + k(mod\ 26)$ and $13 \equiv 19a + k(mod\ 26)$. Solving this system, $a \equiv 3(mod\ 26)$ and $k \equiv 8(mod\ 26)$. Since (3, 26) = 1, this yields a valid cipher $C \equiv 3P + 8(mod\ 26)$. Then $P \equiv 9C + 6(mod\ 26)$.

Ciphertext letter	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
	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Plaintext letter	06	15	24	07	16	25	08	17	00	09	18	01	10	19	02	11	20	03	12	21	04	13	22	05	14	23
	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X

Using this table, we can translate the given ciphertext message as POVER TYIST HEPAR ENTOF REVOL UTION ANDCR IME, that is, POVERTY IS THE PARENT OF REVOLUTION AND CRIME.

Vigenere Ciphers: The Vigenere cryptosystem employs a keyword $w_1w_2 \ldots w_n$ of length n and n shift ciphers $C \equiv P_i + k_i(mod\ 26)$ to each block length n, where k_i is the ordinal number of the letter w_i and $1 \leq i \leq n$.

For example, using the keyword CIPHER and a Vigenere cipher, let us encrypt the message CRYPTOGRAPHY IS FUN. Since the ordinal numbers of the letters C, I, P, H, E, and R are 02, 08, 15, 07, 04 and 17, respectively, they serve as the shift factors for each shift cipher for every block. So the six shift ciphers are $C \equiv P + k(mod\ 26)$, where k = 2, 8, 15, 7, 4 and 17.

Since the keyword is a six-letter word, first we group the letters of the plaintext into blocks of length six: CRYPTO GRAPHY ISFUN.

Now apply the ith cipher to the letter w_i in each block, where $1 \leq i \leq n$. For instance, consider the first CRYPTO. Since the ordinal number are 02, 17, 24, 15, 19 and 14, respectively, add to them the key values 2, 8, 15, 7, 4 and 17 in that order modulo 26. The resulting numbers are 4, 25, 13, 22, 23 and 4, and the corresponding letters are E, Z, N, W, X, and F, respectively, so the first ciphertext block is EZNWXF. Thus the resulting ciphertext is EZNWXF IZPWLP KAUBR.

Hill Cipher: The above cryptosystems are very weak in the sense they can be easily cryptanalyzed. Let us try block ciphers of length 2 and they are called digraphs. In such a system, we group the letters of the plaintext into blocks of length 2, adding a dummy letter X at the end, if necessary, to make all blocks of the same length, and then replace each letter with its ordinal number. Each plaintext block P_1P_2 is then replaced by a numeric ciphertext block C_1C_2, where C_1 and C_2 are different linear combinations of P_1 and P_2 modulo 26:

$$C_1 \equiv aP_1 + bP_2(mod\ 26)$$
$$C_2 \equiv cP_1 + dP_2(mod\ 26) \quad (1)$$

where ($ad - bc$, 26) = 1. This condition is necessary to uniquely solve the linear system of P_1 and P_2. Then we translate each number into a ciphertext letter, the resulting text is the ciphertext.

The following example illustrates this algorithm.

Using the 2 x 2 linear system

$$C_1 \equiv 5P_1 + 13P_2(mod\ 26)$$
$$C_2 \equiv 3P_1 + 18P_2(mod\ 26). \quad (2)$$

encipher the message SLOW AND STEADY WINS THE RACE.

SOLUTION

Step 1 Assemble the plaintext into blocks of length two:

SL OW AN DS TE AD YW IN ST HE RA CE

Step 2 Replace each letter by its cardinal number*:*

18 11 14 22 00 13 03 18 19 04 00 03
24 22 08 13 18 19 07 04 17 00 02 04

Step 3 Using the linear system (2), convert each block into a ciphertext numeric block*:*

When $P_1 = 18$ and $P_2 = 11$, we have

$$C_1 \equiv 5\cdot 18 + 13\cdot 11 \equiv 25 (mod\ 26)$$
$$C_2 \equiv 3\cdot 18 + 18\cdot 11 \equiv 18 (mod\ 26)$$

So the first block 18 11 is converted into 25 18. Transforming the other blocks in a similar fashion yields the numeric string.

25 18 18 22 13 00 15 21 17 25 13 02
16 00 01 24 25 06 09 15 07 25 10 00

Step 4 Translate the numbers into letters.

The resulting ciphertext is ZS SW NA PV RZ NC QA BY ZG JP HZ KA.

Matrices are useful in the study of Hill cryptosystems. For example, that the linear system can be written as

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} \equiv \begin{bmatrix} 5 & 13 \\ 3 & 18 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} (mod\ 26).$$

Since $\Delta = \begin{vmatrix} 5 & 13 \\ 3 & 18 \end{vmatrix} = 51$ and $(51, 26) = 1$, the matrix $\begin{bmatrix} 5 & 13 \\ 3 & 18 \end{bmatrix}$ is invertible modulo 26, with inverse $\begin{bmatrix} 8 & 13 \\ 3 & 21 \end{bmatrix}$ modulo 26. So the deciphering procedure can be effected using the congruence

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \equiv \begin{bmatrix} 8 & 13 \\ 3 & 21 \end{bmatrix} \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} (mod\ 26) \qquad (3)$$

as the following example demonstrates.

Using congruence (3), let us decipher the ciphertext

ZS SW NA PV RZ NC QA BY ZG JP HZ KA

Translating the ciphertext letters into numbers, we get

25 18 18 22 13 00 15 21 17 25 13 02
16 00 01 24 25 06 09 15 07 25 10 00

The plaintext numbers corresponding to the block 25 18 are given by

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \equiv \begin{bmatrix} 8 & 13 \\ 3 & 21 \end{bmatrix} \begin{bmatrix} 25 \\ 18 \end{bmatrix} \equiv \begin{bmatrix} 18 \\ 11 \end{bmatrix} (mod\ 26)$$

So $P_1 = 18$ and $P_2 = 11$. The other blocks can be converted similarly.

It is obvious from the preceding two examples that the size of a block can be any size $n \geq 2$, and that the enciphering and deciphering tasks can be accomplished by choosing an *n*x*n* enciphering matrix A modulo 26 such that $(|A|, 26) = 1$, where $|A|$ denotes the determinant of *A*. Let $P_1, P_2, \ldots, P_n$ be the ordinal numbers of an arbitrary plaintext block and $C_1, C_2, \ldots, C_n$ the corresponding ciphertext numbers. Let

$$P = \begin{bmatrix} P_1 \\ P_2 \\ \vdots \\ P_n \end{bmatrix} \text{ and } C = \begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ C_n \end{bmatrix}.$$

The congruence $C \equiv AP (mod\ 26)$ providing the enciphering transformation.

The RSA Public Key Crypto-System

Let *p* and *q* be distinct large primes and let *n* be their product. Assume that we also have two integers, *d* (for decryption) and *e* (for encryption) such that

$$d \times e \equiv 1\ (mod\ \phi(n)).$$

The integers *n* and *e* are made public, while *p,q* and *d* are kept secret.

Let *M* be the message to be sent where *M* is a positive integer less than and relatively prime to *n*. If we keep *M* less than both *p* and *q*, then we will be safe. In practice, it is enough to keep *M* less than *n* for the probability than a random

M is divisible by *p* or *q* is so small as to be negligible. A plaintext message is easily converted to a number by using, say,

Blank = 99, *A* = 10, *B* = 11, ⋯, *Z* = 35,

So that HELLO becomes 1714212124. If necessary, the message can be broken into blocks of smaller messages: 17142 12124.

The encoder computes and sends the number

$$E = M^e \text{ MOD } n.$$

To decode, we simply compute

$$E^d \text{ MOD } n.$$

By Theorem 3.4 and our equation (4.1) we have that

$$E^d \equiv (M^e)^d \equiv M^{e \times d} \equiv M^{(\text{multiple of } \phi(n)) + 1} \pmod{n}$$
$$\equiv 1 \times M \equiv M \pmod{n}.$$

Since *M* and E^d MOD *n* both lie between 0 and *n*, they must be equal.

If *e* has been chosen relatively prime to $\phi(n)$, then we know that there exists *d*, uniquely such that

$$e \times d \equiv 1 \pmod{\phi(n)}.$$

As we shall prove later in this chapter, if we know the factorization of *n*, namely $n = p \times q$ where *p* and *q* are distinct primes, then we can easily compute $\phi(n)$ by

$$\phi(n) = (p - 1) \times (q - 1).$$

There is no simpler way of computing (n). In fact, knowing ϕ (*n*) equivalent to knowing the factorization becase we can find $p + q$:

$$p + q = n - \phi(n) + 1 = p \times q - (p \times q - p - q + 1) + 1,$$

and the $p - q$ is

$$p - q = \sqrt{(p+q)^2 - 4n} = \sqrt{p^2 + 2p \times q + q^2 - 4p \times q}$$
$$= \sqrt{p^2 - 2p \times q + q^2},$$

and finally:

$$p = \frac{[(p+q) + (p-q)]}{2}, \qquad q = \frac{[(p+q) - (p-q)]}{2}$$

The problem of finding *d*, the decryption key, has been reduced to finding the factorization of *n*.

For this example, the keys were generated as follows:

1. Select two prime numbers, $p = 17$ and $q = 11$.
2. Calculate $n = pq = 17 \times 11 = 187$.
3. Calculate $\phi(n) = (p - 1)(q - 1) = 16 \times 10 = 160$.
4. Select *e* such that *e* is relatively prime to $\phi(n) = 160$ and less than $\phi(n)$; we choose $e = 7$.
5. Determine *d* such that $de \equiv 1 \pmod{160}$ and $d < 160$.

The correct value is $d = 23$, because $23 \times 7 = 161 = (1 \times 160) + 1$; *d* can be calculated using the extended Euclid's algorithm. The resulting keys are public key $PU = \{7, 187\}$ and private key $PR = \{23, 187\}$. The example shows the use of these keys for a plaintext input of $M = 88$.

For encryption, we need to calculate $C = 887 \text{ mod } 187$. Exploiting the properties of modular arithmetic, we can do this as follows:

$88^7 \text{ mod } 187 = [(88^4 \text{ mod } 187) \times (88^2 \text{ mod } 187) \times (88^1 \text{ mod } 187)] \text{ mod } 187$
$88^1 \text{ mod } 187 = 88$
$88^2 \text{ mod } 187 = 7744 \text{ mod } 187 = 77$
$88^4 \text{ mod } 187 = 59{,}969{,}536 \text{ mod } 187 = 132$
$88^7 \text{ mod } 187 = (88 \times 77 \times 132) \text{ mod } 187 = 894{,}432 \text{ mod } 187 = 11$

For decryption, we calculate $M = 11^{23} \text{ mod } 187$:
$11^{23} \text{ mod } 187 = [(11^1 \text{ mod } 187) \times (11^2 \text{ mod } 187) \times (11^4 \text{ mod } 187) \times (11^8 \text{ mod } 187) \times (11^8 \text{ mod } 187)] \text{ mod } 187$
$11^1 \text{ mod } 187 = 11$
$11^2 \text{ mod } 187 = 121$
$11^4 \text{ mod } 187 = 14{,}641 \text{ mod } 187 = 55$
$11^8 \text{ mod } 187 = 214{,}358{,}881 \text{ mod } 187 = 33$
$11^{23} \text{ mod } 187 = (11 \times 121 \times 55 \times 33 \times 33) \text{ mod } 187 = 79{,}720{,}245 \text{ mod } 187 = 88$

The Security of RSA

Four possible approaches to attacking the RSA algorithm are

- Brute force: This involves trying all possible private keys.
- Mathematical attacks: There are several approaches, all equivalent in effort to factoring the product of two primes.
- Timing attacks: These depend on the running time of the decryption algorithm.
- Chosen ciphertext attacks: This type of attack exploits properties of the RSA algorithm.

The defense against the brute-force approach is, to use a large key space. Thus, larger the number of digits in *d*, the better. However, because the calculations involved, both in key generation and in encryption/decryption, are complex, the larger the size of the key, the slower the system will run.

THE FACTORING PROBLEM We can identify three approaches to attacking RSA mathematically.

1. Factor *n* into its two prime factors. This enables calculation of $\phi(n) = (p - 1) \times (q - 1)$, which in turn enables determination of $d \equiv e^{-1} \pmod{\phi(n)}$.
2. Determine $\phi(n)$ directly, without first determining p and q. Again, this enables determination of $d \equiv e^{-1} \pmod{\phi(n)}$.
3. Determine d directly, without first determining $\phi(n)$.

REFERENCE

[1] Elementary Number Theory, David M. Burton, McGraw Hill Publication
[2] Elementary Number Theory with Applications, Thomas Koshy, Elsevier
[3] Elementary Number Theory and its Applications, Kenneth H. Rosen, Addison Wesley