Discrete Mathematics

Lecture 8

Introduction to Cryptography 2

Lecturer: Kahenya N.P

Introduction to lecture 8

This is a continuation to lecture 7 on introduction to cryptography. This lecture will delve into block ciphers and RSA.

References

These lecture notes have been derived from the following sources (Koman et al., 2001; Rosen, 2011, 2012).

Intended Learning Outcomes

At the end of this lecture, you will be able to;

(i) Explain key terms used in cryptography.

(ii) Solve problems involving block ciphers and RSA.

Introduction

Shift and Block ciphers are examples of symmetric key ciphers. Symmetric-key cryptography are those that both the sender and the receiver share the same key, that is, encrypting and decrypting keys are related in an easily computable way. Identifying the encrypting key one can easily compute the decrypting key. Since ideally the ciphers uses the same key for encryption and decryption. This poses a disadvantage. Symmetric-key cryptosystems are also referred to a private key cryptosystem.

On the other hand, we have asymmetric key cryptography in which two different keys, a public key and a private key are used. However, the keys are different but mathematically related. In public-key encryption systems, the public key is used for encryption while the private key is used for decryption. Knowing how to send encrypted messages does not help decrypt the message. Everyone has the encryption key, but the decryption key is secret. Examples of public cryptosystems is the RSA and Diffle-Hellman algorithms.

Block ciphers

Shift ciphers and affine ciphers are monoalphabetic ciphers since they proceed by replacing each letter of the alphabet by another letter in the alphabet. Such ciphers are weak and vulnerable to brute-force attacks due to the analysis of letter frequency used. One alternative to use blocks of letters or characters i.e., block ciphers.

A block cipher encrypts information in blocks. A block may be of a certain fixed size that is used informally in encrypting a set of data. The algorithm used encrypt the block simultaneously instead of individual bits of the block.

Modern block ciphers encrypt data in fixed-size blocks of either 64 bits or 128 bits. For example, the Data Encryption Standard DES, and the Advanced Encryption Standard AES are block ciphers.

Further readings: Block cipher mode of operations on how blocks are encrypted (What is a block cipher? (techtarget.com)).

Transposition cipher

It is an example of block cipher that use the key as a permutation μ of the set {1,2,3, … n} for some positive integers n. To encrypt a message, we first split its letters into blocks of size n.

In case the number of letters is not divisible by n a random letter(s) (dummy) is added at the end to fill out the final block. The procedure is to encrypt the block;

$p_1p_2p_3 \ \dots \ p_n$ as $c_1c_2c_3 \ \dots \ c_n = p_{\mu(1)}p_{\mu(2)}p_{\mu(3)} \cdots p_{\mu(n)}$

The procedure of decrypting the ciphertext block $c_1c_2c_3 \ \dots \ c_n$ we use the permutation μ^{-1} i.e., the inverse of permutation μ

Example 1: Use the transposition cipher based on the permutation p of the set {1 2 3 4 5} with p(1) = 2, p(2) = 5, p(3) = 1, p(4) = 3 and p(5) = 4 to encrypt the plaintext message;

GREAT MIGRATIONS

Solution: We split the plaintext into blocks of 5 letters to obtain;

GREAT MIGRA TIONS

To get; EGATR GMRAI OTNSI

Example 2: Use the transposition cipher based on the permutation $\mathrm{p} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$ of the set $\{1,2,3,4,5\}$ to encrypt the plaintext message:

THE HORNETS AND WASP HAD A CRAZY ENCOUNTER

Solution: We split the plaintext into blocks of 5 letters to obtain;

THEHO RNETS ANDWA SPHAD ACRAZ YENCO UNTER

We encrypt to get; EHOTH ETSRN DWAAN HADSP RAZAC NCOYE TERUN

Example 3: Using the transposition cipher based on the encrypting function represented by the permutation $\mathrm{p} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$, decrypt the ciphertext:

TYLOEGOUORPIDRSLEIATEODNMEVAELATLHP.

Solution: The decrypting function is $\mathrm{p} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$ We split the ciphertext into blocks of 5 letters to obtain;

TYLOE GOUOR PIDRS LEIAT EODNM EVAEL ATLHP

Decrypting the text, we obtain; LET YOUR GOOD SPIRIT LEAD ME ON A LEVEL PATH.

Hill cipher

Hill cipher is a polygraphic substitution cipher. The plaintext is grouped into blocks of say 2 letters that are then encrypted. Each block of n letters is multiplied by an invertible $n \times n$ matrix modulo 26, chosen randomly. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption. The determinant of the chosen matrix should be relatively prime to 26.

Example 1: Encrypt the plaintext: *the blue eagle*

Solution: Split the message into blocks of 2 letters (add a dummy letter at the end if necessary).

TH EB LU EE AG LE

Translate into their numerical equivalent i.e.

19,7, 4,1 11,20 4,4 0,6 11,4

To get the ciphertext CT we use a key which is a $n \times n$ matrix of order 2 i.e.

$$\mathrm{CT} = \mathrm{A[PT]mod\ 26\ where\ PT\ is\ the\ plaintext}$$

The key matrix A should be invertible modulo 26 and $(\det A, 26) = 1$.

We can let our key matrix be $\begin{pmatrix} 3 & 7 \\ 4 & 11 \end{pmatrix}$. Note that the determinant is 5.

Hence the first block of 2 letters becomes;

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 3 & 7 \\ 4 & 11 \end{pmatrix} \begin{pmatrix} 19 \\ 7 \end{pmatrix} \bmod 26 = \begin{pmatrix} 2 \\ 23 \end{pmatrix}$$

$$\Rightarrow 2 = C, 23 = X$$

We can find for the rest;

$$\left(\begin{pmatrix} c_i \\ c_j \end{pmatrix} \right) = \begin{pmatrix} 3 & 7 \\ 4 & 11 \end{pmatrix} \begin{pmatrix} 4 & 11 & 4 & 0 & 11 \\ 1 & 20 & 4 & 6 & 4 \end{pmatrix} \bmod 26 = \begin{pmatrix} 19 & 17 & 14 & 16 & 9 \\ 1 & 4 & 8 & 14 & 10 \end{pmatrix}$$

i.e. TB RE OI QO JK

To decrypt we use the function;

$$PT = A^{-1}(CT) \bmod 26$$

Where A^{-1} is the inverse of A modulo 26. It can be shown that $A^{-1} = \frac{1}{5}\begin{pmatrix} 11 & -7 \\ -4 & 3 \end{pmatrix}$

To get the plaintext from the ciphertext CX;

$$PT = A^{-1}(CT) \bmod 26 = \frac{1}{5}\begin{pmatrix} 11 & -7 \\ -4 & 3 \end{pmatrix}\begin{pmatrix} 2 \\ 23 \end{pmatrix} \bmod 26$$

$$= \overline{5}\begin{pmatrix} -139 \\ 61 \end{pmatrix} \bmod 26$$

Note that the inverse of 5 mod 26 is 21.

$$= 21\begin{pmatrix} 17 \\ 9 \end{pmatrix} \bmod 26 \; = \begin{pmatrix} 19 \\ 7 \end{pmatrix} \bmod 26$$

Clearly our plaintext was T and H.

Remark 1: The Hill ciphers are still vulnerable based on the frequencies of the blocks.

RSA cryptosystem

RSA is a type of asymmetric encryption that uses private and public keys. The keys are different but related. It is an example of a public key cryptosystem by Rivest, Shamir and Adleman (RSA) 1976. The two keys can be used to encrypt and decrypt a message i.e., commutative keys. The algorithm security is based on the premise that it is difficulty to factor large integers (semi prime numbers) that it uses. Again, the strength of the encryption is dependent on the key size too.

In the RSA system each individual has an encryption key (n, e) where;

$$n = pq$$

That is, the product of two large primes p and q with 200 digits plus, and

e is an exponent that is relatively prime to $(p - 1)(q - 1)$.

Note that to produce a usable key two large numbers must be found. This is normally not easy. The product of these two primes (400 + digits) cannot easily be factored within a reasonable time.

To encrypt a message using the key (n, e) we use the function $c = M^e \bmod n$.

To decrypt a message using the key (n,d) we use the function $p = M^d \bmod n$.

Example 1: Steps for RSA encryption

First is to generate the keys

- Choose two prime numbers p and q say $p = 11, q = 3$
- Find $n = pq$ i.e., $n = 11 \times 3 = 33$ (to get a semi-prime number).
- Calculate totient $m = (p - 1)(q - 1)$ i.e., $10 \times 2 = 20$

Next we select a *public key* e must be:

- a prime
- less than the totient, and
- not be a factor of the totient.

We can select 3 since it satisfies the above.

We also select a private key d that must satisfy the following:

- the product of d and e gives a remainder 1 when divided by totient m (That is, the numbers are relatively prime). We can select $d = 7$ and since our $e = 3$ then $ed = 21$ which is $1 \pmod{20}$ i.e., gcd (ed, m) = 1.
  Recall: $1 \equiv ed \pmod{n} \Rightarrow 1 \equiv km + ed$

Publish public key $(n, e) = (33,3)$

To encrypt we use the function; $c = p^e \pmod{n}$.

To decrypt we use the function; $p = c^d \pmod{n}$.

We next use the public key to encrypt letter j that has a value 9 i.e., $j = 9$.

We use the encryption function to get;

$$c = 9^3 \pmod{33} = 3$$

the letter j will be encrypted as d.

To decrypt letter $d = 3$ we use the decrypting function with private key $(n, d) = (33, 7)$ i.e.

$$p = 3^7 \pmod{33} = 9$$

Since the keys are commutative we can verify with the example above.

We use the private key 7 to encrypt i.e., $\mathrm{c} = 3^7 \mathrm{mod}\ 33 = 9$

We use the public key 3 to decrypt i.e., $\mathrm{p} = 9^3 \mathrm{mod}\ 33 = 3$

Example 2: Let choose two primes $p = 23$ and $q = 31 \Rightarrow n = pq = 713$

Our totient $m = (23-1)(31-1) = 22 \times 30 = 660$

Let the public key $e = 7$ and to get private key d then $ed = 1 \bmod 660$

$$7\mathrm{d} = 1 \bmod 660$$

$$660 = 94 \cdot 7 + 2$$

$$7 = 3 \cdot 2 + 1$$

$$\therefore 1 = 7 - 3(2) = 7 - 3[660 - 94(7)] = 283(7) - 3(660)$$

Introducing mod 660 we get;

$$283 \cdot 7 \bmod 660 - 3 \cdot 660 \bmod 660 = 1 \bmod 660$$

$$283 \cdot 7 = 1 \bmod 660$$

$$\Rightarrow d = 283$$

We encrypt the value 34 with the public key i.e., $c = 34^7 mod\ 713 = 513$

We can decrypt 513 with the private key 283 to verify if we can get our message 34 back i.e.

$$\mathrm{p} = 513^{283} \mathrm{mod}\ 713 = 34$$

Example 3: Let choose two primes $p = 37$ and $q = 53 \Rightarrow n = pq = 37 \times 53 = 1961$

Our totient $m = (37-1)(53-1) = 1872$

Let the public key $e = 11$

To get the private key d we need to have $ed = 1\ mod\ 1872$

$$11d = 1\ mod\ 1872$$

$$1872 = 11 \cdot 170 + 2$$

$$11 = 5 \cdot 2 + 1$$

$$\therefore 1 = 11 - 5(2) = 11 - 5[1872 - 170(11)] = 851(11) - 5(1872)$$

Introducing mod 1872 to get;

$$851 \cdot 11 \bmod 1872 - 5 \cdot 1872 \bmod 872 = 1 \bmod 1872$$

$$851 \cdot 11 \bmod 1872 = 1 \bmod 1872$$

Therefore, the inverse of 11 mod 1872 is 851$\therefore \mathrm{d} = 851$

Let encrypt the message; HURT

We block the message into blocks of two letters i.e.

HU RT

Note that we can also code blank space 00, A=01, B= 02 …Z=26

Using values, the block is; 0821 1820

(NB: No block should exceed $n = 1961$).

Encrypting the first block to get;

$$821^{11} \bmod 1961 = 1233$$

Encrypting the second block to get;

$$1820^{11} \bmod 1961 = 0419$$

$\Rightarrow 1233\ 0419 = \text{LFDS}$

$(33 \bmod 27 = 6 = \text{F})$

We can decrypt to confirm if the private key is working

$$1233^{851} mod\ 1961 = 821$$

$$419^{851} mod\ 1961 = 1820$$

Exercise

1) Explain the Diffie-Hellman key exchange.
2) Explain the operation of digital signature
3) Using the transposition cipher based on the permutation of the set {1,2,3,4,5} with $p(1) = 5, p(2) = 3, p(3) = 4, p(4) = 1, p(5) = 2$, to;
    a. Encrypt the plaintext; DUSTY ROAD GOSPEL MUSIC
    b. Decrypt the ciphertext; NJIEXDTYEOBRISHFRSSAIDMMONAHIC
4) Attempt exercise (Rosen, 2012, p. 304)

References

Koman, B., Busby, R., & Ross, S. (2001). *Discrete Mathematical Structures*. Prentice-Hall.
Rosen, K. (2011). *Elementary Number Theory and Its Application* (6th ed.). Person.
Rosen, K. (2012). *Discrete mathematics and its application* (7th ed.). McGraw-Hill.