EE 418: Handout #1

Information Security, Classical Cryptosystems, and Cryptanalysis

Lecture notes of Professor Radha Poovendran
Network Security Lab (NSL)
Dept. of Electrical and Computer Engineering
University of Washington

Abstract. Introduction to the main concepts of information security and outline of its objectives. Common terminology used throughout the course is also being introduced. Classical monoalphabetic cryptosystems including Shift cipher, Substitution cipher and the Affine cipher are reviewed. Readings from Chapters one and two of the fourth edition of D. Stinson.

1 Information Security

Information security has existed for thousands of years in many forms, and is an integral part of our everyday lives beyond the scope of computers and digital communications.

Examples:

- Hieroglyphics in ancient Egypt – A form of encryption, since only a handful of priests could read the writings.
- Money – Watermarks (printed patterns and hidden symbols) make it very hard to counterfeit. Authenticates the source and demonstrates the integrity of the information.
- Signatures in physical documents – The physical signature in a document authenticates the source of the document or verifies someone's endorsement.
- Seal in a letter – Seals and envelopes aim at ensuring information privacy between the sender and the receiver. The privacy mechanism is reactive rather than proactive. Although anyone can open the letter by breaking the seal, they are prohibited from doing so by criminal law.

1.1 Objectives of Information Security

Information security has multiple objectives that have to be satisfied depending on what is the use of the information that is being secured.

1. *Confidentiality*: Restricting access to the information only to authorized entities.
2. *Identity Authentication*: Corroboration of an identity to an entity.
3. *Message Authentication*: Corroboration of a message to an entity, i.e. verifying the source of a message.
4. *Data Integrity*: Ensuring that the information has not been altered by an unauthorized entity.
5. *Non-repudiation*: Preventing the denial of previous commitments or actions (think of a contract).
6. *Authorization*: Conveyance to another entity of official sanction to perform an action.
7. *Certification*: Endorsement of information by a trusted entity.

Figure /reffig:infsec below lists information security objectives.

privacy or confidentiality	keeping information secret from all but those who are authorized to see it.
data integrity	ensuring information has not been altered by unauthorized or unknown means.
entity authentication or identification	corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.).
message authentication	corroborating the source of information; also known as data origin authentication.
signature	a means to bind information to an entity.
authorization	conveyance, to another entity, of official sanction to do or be something.
validation	a means to provide timeliness of authorization to use or manipulate information or resources.
access control	restricting access to resources to privileged entities.
certification	endorsement of information by a trusted entity.
timestamping	recording the time of creation or existence of information.
witnessing	verifying the creation or existence of information by an entity other than the creator.
receipt	acknowledgement that information has been received.
confirmation	acknowledgement that services have been provided.
ownership	a means to provide an entity with the legal right to use or transfer a resource to others.
anonymity	concealing the identity of an entity involved in some process.
non-repudiation	preventing the denial of previous commitments or actions.
revocation	retraction of certification or authorization.

Fig. 1: Objectives of information security. Source: A. J. Menezes, P. C. Van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography,* CRC-Press, 1996.

Cryptography is a mechanism for realizing these security properties. Cryptographic protocols are implementations of cryptographic algorithms.

2 Classical Cryptography

The fundamental objective of cryptography is to enable two parties, often referred to as (**A**)lice and (**B**)ob, to communicate over an insecure (ofter referred to as public) channel in such a way that an eavesdropper (**E**)ve, cannot understand what is being communicated. To prevent Eve from understanding the secret communication, Alice encrypts the messages sent to Bob in a way that only Bob can decrypt. The process of securing two-party communication over an insecure channel is depicted in Figure 2.

In Figure 2 Alice wants to send a message to Bob. This message is known as the "plaintext." Alice encrypts the plaintext using a predetermined key and creates the "ciphertext." The ciphertext is transmitted over the insecure channel to Bob. Using the predetermined encryption key, Bob decrypts the ciphertext and recovers the plaintext. An eavesdropper Eve observing the insecure channel cannot obtain the plaintext from the ciphertext, since it does not know the predetermined key.

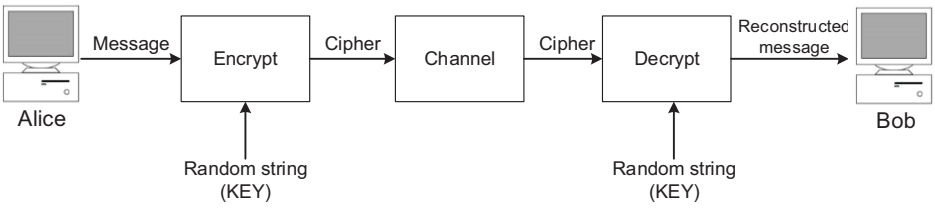

Fig. 2: Schematic of a secure communication over an insecure channel

Before we proceed with cryptographic methods for establishing secure communication over an insecure channel, we define common terminology that will be used throughout the course.

3 Common Terminology

3.1 Secrecy

The quality or condition of being hidden or concealed. *Communication secrecy* is then the condition of communicating secretly.

3.2 Communicating parties

The entities that wish to (secretly) communicate. In the case of two-party communication we refer to them as (**A**)lice and (**B**)ob.

3.3 Communication channel

A *communication channel* is the physical medium over which communication occurs. A channel can be wired (e.g. copper wire, optic fiber) or wireless (e.g. radio).

3.4 Eavesdropper or Adversary

The entity we wish to conceal the information from. The entity is often modeled as an EaVEsdropper referred to as (**E**)ve, passively observing the communication channel. In other cases, the entity may be actively trying to decrypt the communicated information. In the general case, this entity is referred to as Opponent or Adversary.

3.5 Cryptography

Cryptography can be considered as an algorithmic process of designing secrecy systems for securing communication between parties.

3.6 Cryptanalysis

The process of analyzing cryptosystems, for the purpose of breaking the secrecy of the communication.

3.7 Communication modes

The different modes of communication can be classified as follows.

1. *Unicast*: One-to-one or point-to-point communication.
2. *Multicast*: One-to-many or point-to-multipoint communication.
3. *Broadcast*: One-to-any or point-to-any point communication. Multicast is a special case of broadcast communication.

3.8 Plaintext

The information that Alice wants to communicate to Bob. It can be text, numerical data, or anything else.

3.9 Ciphertext

The message that is transmitted over the insecure channel after the plaintext has been encrypted. Decryption of the ciphertext using the correct decryption algorithm and decryption key will produce the corresponding plaintext.

3.10 Encryption/Decryption key

A secret shared by the communicating parties that is used in cryptographic operations.

3.11 Encryption

The process of creating a ciphertext from a plaintext by using an encryption key K and following an encryption rule (algorithm) e_K.

3.12 Decryption

The process of obtaining the plaintext from a ciphertext by using a decryption key K and following a decryption rule (algorithm) d_K.

3.13 Formal description of a cryptosystem

A cryptosystem can be represented in terms of 5 parameters $(\mathscr{P}, \mathscr{C}, \mathscr{K}, \mathscr{E}, \mathscr{D})$.

1. $\mathscr{P}$ is the set of possible plaintexts.
2. $\mathscr{C}$ is the set of possible ciphers.
3. $\mathscr{K}$ is the set of possible keys.
4. $\mathscr{E}$ is the encryption rule set.
5. $\mathscr{D}$ is the decryption rule set.

Let $x \in \mathscr{P}$, $K \in \mathscr{K}$. Encryption is a rule $e_K \in \mathscr{E}$, and decryption is a rule $d_K \in \mathscr{D}$. We require:

$$d_K(e_K(x)) = x. \tag{1}$$

In words, decryption should uniquely recover the original plaintext.

Properties of encryption

- The encryption function e_K must be *injective* (i.e. one-to-one) so that decryption can occur in an unambiguous manner.
- If $\mathscr{P} = \mathscr{C}$, that is, the plaintext and ciphertext spaces are the same, then each encryption is a permutation, that is, it rearranges the elements of the plaintext space.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Table 1: Mapping of alphabets to numerals

3.14 Convention followed in the course and textbook

As shown in the table 1, we can denote the element of any alphabet with corresponding numbers. Throughout the lecture notes, plaintext is indicated by *lowercase* and ciphers are indicated by *UPPERCASE*.

3.15 Example

Suppose that **(A)**lice wants to send a message to **(B)**ob over an insecure channel. A and B do not want this information to be readable by any other parties.

1. *What does A do?*
   (a) A takes plaintext $x = x_1x_2 \dots x_n$ for some integer $n \geq 1$, with $x_i \in \mathscr{P}$, $\forall i$, and encrypts with a key $K \in \mathscr{K}$ using the encryption rule e_K to generate $ciphertext$ (cipher) $Y = Y_1Y_2 \dots Y_n$.
   (b) A transmits the cipher Y over the insecure channel.

2. *What does B do?*
   (a) B knows the key K and the *decryption algorithm* d_K.
   (b) B receives the cipher Y and runs decryption.
   (c) B recovers the plaintext x.

3.16 Alphabet

The set of possible values of x_i in a plaintext $x = x_1x_2 \dots x_n$ is called an alphabet. Examples: The English alphabet consists of 26 letters. The bit alphabet consists of $\{0, 1\}$.

4 Substitution Cipher

The idea of the substitution cipher is to replace each alphabet of the plaintext with an alphabet at an *arbitrary distance*. Formally, we can describe this cryptosystem as follows.

Let $\mathscr{P} = \mathscr{C} = \mathbb{Z}_{26}$. The keyspace $\mathscr{K}$ includes all possible permutations of the 26 symbols, $0, 1, \dots, 25$. For each permutation $\pi \in \mathscr{K}$:

$$y = e_\pi(x) = \pi(x), \tag{2}$$

$$d_\pi(y) = \pi^{-1}(y). \tag{3}$$

π^{-1} denotes inverse permutation to π. Since a key consists of a permutation of the 26 letters, the keyspace is very large including $26! \approx 4.0 \times 10^{26}$. Hence, the key space in the substitution cipher is much larger than the key space of the shift cipher, and a brute force attack (exhaustive) search will take a very long time. We

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

will see that other attacks are feasible against the substitution cipher. For illustration, consider the following permutation π which represents encryption by one of the 26! possible keys.

Given π, we have $e_\pi(a) = \pi(a) = X$, $e_\pi(b) = \pi(b) = N$, and so on. In order to decrypt, we obtain the inverse permutation π^{-1} as follows: re-write the above table, by interchanging the rows, and then sorting the columns such that the first row is in alphabetical order.

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
d	l	r	y	v	o	h	e	z	x	w	p	t	b	g	f	j	q	n	m	u	s	k	a	c	i

Therefore, we have $d_\pi(A) = \pi^{-1}(A) = d$, $d_\pi(B) = \pi^{-1}(B) = l$, and so on.

5 The Permutation Cipher

The idea of the *Permutation Cipher* (Transposition Cipher) cryptosystem is to generate the ciphertext by *altering the positions of the characters* in the plaintext, i.e. by re-arranging them using a permutation. In contrast to the Substitution Cipher, there is no replacement of characters (it is similar to just scrambling the letters of a word). Formally, we describe the Permutation Cipher cryptosystem as follows.

Let $\mathscr{P} = \mathscr{C} = (\mathbb{Z}_{26})^m$, where m is a positive integer. $\mathscr{K}$ includes all permutations of $\{1, ..., m\}$. For each permutation $\pi \in \mathscr{K}$:

$$y = e_\pi(x_1, ..., x_m) = (x_{\pi(1)}, ..., x_{\pi(m)}) \tag{4}$$

$$x = d_\pi(y_1, ..., y_m) = (y_{\pi^{-1}(1)}, ..., y_{\pi^{-1}(m)}). \tag{5}$$

π^{-1} denotes inverse permutation to π. For illustration, consider the following example. Given $m = 6$, and permutation (the key) π is as follows:

j	1	2	3	4	5	6
$\pi(j)$	3	5	1	6	4	2

To obtain π^{-1}, interchange the rows, and sort the columns such that the first row is in ascending order. We obtain:

For encryption, if the plaintext is ***followashore***, we first partition the plaintext into groups of six letters as: ***follow*** | ***ashore***. Using the above key π, we re-arrange each group of six alphabets as: *LOFWLO* | *HRAEOS*. Similarly, the ciphertext can be decrypted using the inverse permutation π^{-1}.

j	1	2	3	4	5	6
$\pi^{-1}(j)$	3	6	1	5	2	4

6 The Quotient Remainder Theorem

Theorem 1. *Given any integer "a" (i.e., $a \in \mathbb{Z}$) and a positive integer "m" (i.e., $m \in \mathbb{Z}^+$), there exists unique integers q and r (i.e., $q, r \in \mathbb{Z}$) such that*

$$a = q \cdot m + r \tag{6}$$

where $0 \leq r < m$. Moreover, q and r are called the quotient and the remainder of "a" with respect to "m", respectively.

7 Modulo Arithmetic

Definition 1. *Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. We write $a \equiv b \pmod{m}$ if m divides $(a - b)$. We can also write $m|(a - b)$ if m divides $(a - b)$. The operator $\equiv$ is called congruence and $a \equiv b \pmod{m}$ is read: "a is congruent to b modulo m." The positive integer m is known as the modulus.*

7.1 Properties of modulo arithmetic

Let $\mathbb{Z}_m$ denote the set of integers $\{0, 1, 2, \ldots, m - 1\}$.

1. $a \equiv b \pmod{m}$ if and only if $a \pmod{m} = b \pmod{m}$, i.e. the remainders of a and b modulo m are equal.
2. Addition is *closed*: for any $a, b \in \mathbb{Z}_m,\ a + b \in \mathbb{Z}_m$.
3. Addition is *commutative*: for any $a, b \in \mathbb{Z}_m, a + b = b + a$.
4. Addition is *associative*: for any $a, b, c \in \mathbb{Z}_m, (a + b) + c = a + (b + c)$.
5. 0 is an additive identity: for any $a \in \mathbb{Z}_m, a + 0 = 0 + a = a$.
6. The *additive inverse* of any $a \in \mathbb{Z}_m$ is $m - a$: that is $a + (m - a) = (m - a) + a = 0,\ \forall a \in \mathbb{Z}_m$.
7. Multiplication is *closed*: for any $a, b \in \mathbb{Z}_m, ab \in \mathbb{Z}_m$.
8. Multiplication is *commutative*: for any $a, b \in \mathbb{Z}_m, ab = ba$.
9. Multiplication is *associative*: for any $a, b, c \in \mathbb{Z}_m, (ab)c = a(bc)$.
10. 1 is the multiplicative identity: for any $a \in \mathbb{Z}_m, a \times 1 = 1 \times a = a$.
11. The *distributive* property is satisfied: for any $a, b, c \in \mathbb{Z}_m, (a + b)c = (ac) + (bc)$ and $a(b + c) = (ab) + (ac)$.

Properties 1, 3-5, say that $\mathbb{Z}_m$ forms a *group*. Since property 2 also holds, the group is called an *abelian group*. Properties 1-10 make $\mathbb{Z}_m$ a *ring*.

We can also define subtraction in $\mathbb{Z}_m$ as $(a - b) \pmod{m}$.

8 Shift Cipher

The idea used in the *shift cipher* cryptosystem is to replace each letter in an alphabet by another letter at a *fixed distance* K from it. As an example, let $K = 3$[1] and the plaintext be *shift*. Assume each letter is shifted right (or left) by 3 places. We then get *VKLIW* as the cipher (for a right shift).

More formally, we can describe this shift cipher as follows. Associate each integer $0, \ldots, 25$ with $A, B, ..., Z$. The key K can be any integer with $0 \leq K \leq 25$. We can then write:

$$\mathscr{P} = \mathscr{C} = \mathscr{K} = \mathbb{Z}_{26}.$$
For $0 \leq K \leq 25$,

$$y = e_K(x) = (x + K) \bmod 26, \tag{7}$$
$$x = d_K(y) = (y - K) \bmod 26. \tag{8}$$

8.1 Is the Shift Cipher Secure?

Brute force attack: Assume Eve knows only the ciphertext $VKLIW$. Eve also knows that a shift cipher algorithm is used for encryption. Given the small cardinality of the key space, Eve can try all the possible 26 shifts in right direction, as shown in Fig. 3. Upon shifting, the following plaintexts are obtained:
$vkliw \overset{1^{st}left\ shift}{\longrightarrow} ujkhv \overset{2^{nd}left\ shift}{\longrightarrow} tijgu \overset{3^{rd}left\ shift}{\longrightarrow} shift$, and so on. Since, "shift" is the only dictionary word in the list of 26 possible words in Fig. 3, Eve assumes that it is indeed the plaintext that was encrypted. Therefore, Eve can also infer the original key $K = 3$.

9 Affine Cipher

The idea of the Affine cipher is to first *scale* and then shift, which is known as the *affine transformation*.

$$y = e_K(x) = (ax + b) \mod 26, \tag{9}$$
$$d_K(y) = a^{-1}(y - b) \mod 26. \tag{10}$$

In this scheme, the pair (a, b) denotes the cryptographic key K used for encryption/decryption.

Here we need to know which (a, b) are valid keys that yield an injective encryption function. Note that we need to know a^{-1} for decryption. Also if $a = 1$, the affine cipher becomes identical to the shift cipher.

9.1 Decryption of the Affine Cipher

Definition 2. *The modular multiplicative inverse of an integer $a \in \mathbb{Z}_m$ modulo m, denoted as $a^{-1} \mod m$, is an element $a' \in \mathbb{Z}_m$ such that $aa' \equiv a'a \equiv 1 \pmod m$.*

If m is prime, every non-zero element of $\mathbb{Z}_m$ has a multiplicative inverse. The modular multiplicative inverse of an integer $a \in \mathbb{Z}_m$ can be found using either the *Extended Euclidean Algorithm,* or the *Direct*

[1] For $K = 3$, the shift cipher is often called the Caesar Cipher, since it was allegedly used by Julius Caesar.

Attack on Shift Cipher: *Given, VKLIW is the cipher, find the plaintext.*

Using correspondence between alphabetic characters and residues modulo 26 given in the notes, we get for the given cipher, VKLIW, the sequence of numbers as, 21 10 11 8 22
Following values are then obtained by subtracting 0 <= K <=25 (and reducing modulo 26) from each value in the above sequence.

Residues modulo 26	Corresponding Plaintext
21 10 11 8 22	**vkliw**
20 9 10 7 21	ujkhv
19 8 9 6 20	tijgu
18 7 8 5 19	**shift**
17 6 7 4 18	rghes
16 5 6 3 17	qfgdr
15 4 5 2 16	pefcq
14 3 4 1 15	odebp
13 2 3 0 14	ncdao
12 1 2 25 13	mbczn
11 0 1 24 12	labym
10 25 0 23 11	kzaxl
9 24 25 22 10	jyzwk
8 23 24 21 9	ixyvj
7 22 23 20 8	hwxui
6 21 22 19 7	gvwth
5 20 21 18 6	fuvsg
4 19 20 17 5	eturf
3 18 19 16 4	dstqe
2 17 18 15 3	crspd
1 16 17 14 2	bqroc
0 15 16 13 1	apqnb
25 14 15 12 0	zopma
24 13 14 11 25	ynolz
23 12 13 10 24	xmnky
22 11 12 9 23	wlmjx

Fig. 3: Brute force attack on the shift cipher.

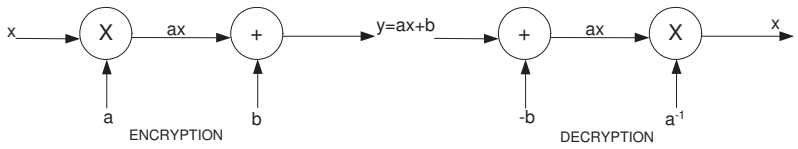

Fig. 4: Schematic of the affine cipher cryptosystem

Modular Exponentiation method. Given the multiplicative inverse, the congruence $y \equiv ax + b \pmod{26}$ can be solved for x as follows.

$$ax \equiv y - b \pmod{26}, \tag{11}$$
$$a^{-1}(ax) \equiv a^{-1}(y - b) \pmod{26}, \tag{12}$$
$$a^{-1}(ax) \equiv (a^{-1}a)x \equiv 1x \equiv x \pmod{26}, \tag{13}$$
$$x = a^{-1}(y - b) \mod 26. \tag{14}$$

An example of an affine cipher.

Let $a = 9$ and $b = 3$. Let the plaintext be d that corresponds to the numerical value 3, based on table 1.

$$e_K(d) = (9 \times 3 + 3) \bmod 26 = 4. \tag{15}$$

For the decryption part,

$$d_K(4) = a^{-1}(4 - b) \bmod 26 = 9^{-1}(4 - 3) \bmod 26 = 9^{-1} \pmod{26} = 3, \tag{16}$$

which is the multiplicative inverse of $9 \pmod{26}$, i.e. $9 \times 3 \equiv 1 \pmod{26}$.

9.2 Problem with choice of a

Not all choices of a have a multiplicative inverse. As an example, consider the case where $a = 13$ and $b = 3$. Assume the plaintext is the word *busted*. Using the table above, we can compute cipher for $busted$ as follows.

$$e_K(1) = (13 \times 1 + 3) \bmod 26 = 16 = Q. \tag{17}$$
$$e_K(20) = (13 \times 20 + 3) \bmod 26 = 3 = D. \tag{18}$$
$$e_K(18) = (13 \times 18 + 3) \bmod 26 = 3 = D. \tag{19}$$
$$e_K(19) = (13 \times 19 + 3) \bmod 26 = 16 = Q. \tag{20}$$
$$e_K(4) = (13 \times 4 + 3) \bmod 26 = 3 = D. \tag{21}$$
$$e_K(3) = (13 \times 3 + 3) \bmod 26 = 16 = Q. \tag{22}$$

i.e. $busted \longrightarrow QDDQDQ$.

Since multiple plaintexts will result in this ciphertext (for instance, the word *dealer* also encrypts to $QDDQDQ$), no unique decryption is possible here. This is due to the fact that $a = 13$ does not have a multiplicative inverse in $\mathbb{Z}_{26}$. For your interest you can also work out the example for $a = 2$, and see that affine cipher does not work. It is therefore important to characterize the integers that have multiplicative inverses mod 26.

We now introduce the concept of *greatest common divisor*. Given two integers a and b, the greatest common divisor of a and b (denoted $\gcd(a,b)$) is equal to the largest integer c that divides both a and b.

First, note that an integer a has an inverse mod m if and only if there exist p and q such that $ap+mq=1$. We have $1 = ap + mq \equiv ap \bmod m$, which implies that a has multiplicative inverse p mod m. On the other hand, $r \equiv 1 \bmod m$ if and only if $r + bm = 1$ for some b, implying that $ap \equiv 1 \bmod m$ if and only if $ap + mq = 1$ for some q. This, in turn, can only happen when $\gcd(a,m) = 1$.

To see why, let $c = \gcd(a,m)$ and suppose $c > 1$. Then there exist positive integers α, β satisfying $a = \alpha c$ and $m = \beta c$. If $ap + mq = 1$ for some p, q, then $pc\alpha + qc\beta = 1$, hence $c(p\alpha + q\beta) = 1$. This is a contradiction since there are no positive integers that divide 1 (except 1 itself).

The other direction is also true: if $\gcd(a,m) = 1$, then there exist integers p, q satisfying $ap + mq = 1$. These integers can be computed using the extended Euclidean algorithm. The integer p will be the multiplicative inverse of a mod m.

Theorem 2. *If $gcd(a,m) = 1$ then $ax \equiv y \pmod m$ has a unique solution x.*

Example: Given $m = 26$, for $a = 13$ we have $gcd(13, 26) = 13 \neq 1$. Also if $a = 2$ then $gcd(2, 26) = 2$.

But for $a = 9$, $gcd(9, 26) = 1$ and hence the affine cipher works. Similarly for $a = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$ we have $gcd(a, 26) = 1$. Hence, a can take a total of 12 values with unique inverses in $\mathbb{Z}_{26}$, and b can take any of the 26 values in $\mathbb{Z}_{26}$. Therefore the key space is limited to $12 \times 26 = 312$ values for K, and a brute force attack (exhaustive search is possible).

9.3 Computation of the cardinality of the key space for the Affine Cipher

Definition 3. *An integer $p > 1$ is prime if it has no positive divisors other than 1 and p.*

Theorem 3 (Unique Factorization). *For any integer m, there exists an integer n, a set of distinct primes $p_1, \ldots, p_n$, and a set of integers $e_1, \ldots, e_n$ satisfying*

$$m = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \tag{23}$$

Furthermore, the sequences $p_1, \ldots, p_n$ and $e_1, \ldots, e_n$ are unique up to reordering of the p_i's.

Example: For $m = 192$,

$$432 = 2^4 \times 3^3. \tag{24}$$

This factorization is unique up to a rearrangement of the terms on the right hand side (i.e., we can write $3^3 \times 2^4$ instead).

Definition 4. *Two integers $a \geq 1$ and $m \geq 2$ are said to be relatively prime if $gcd(a,m) = 1$. The number of integers in $\mathbb{Z}_m$ that are relatively prime to m is known as the Euler-phi function, denoted by $\phi(m)$.*

Theorem 4. *Let*

$$m = \prod_{i=1}^{n} p_i^{e_i}, \tag{25}$$

where p_i are distinct primes and $e_i > 0, 1 \leq i \leq n$. Then

$$\phi(m) = \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i - 1}). \tag{26}$$

Based on Theorem 2, the cardinality of the key space for the Affine Cipher is $m\phi(m)$.

Example: For $m = 60$

$$60 = 2^2 \times 3^1 \times 5^1, \tag{27}$$

and,

$$\phi(m) = (4-2) \times (3-1) \times (5-1) = 16. \tag{28}$$

The cardinality of the key space $60 \times 16 = 960$ keys.