Computer Network Security

Lesson 7

Cryptography I

Lecturer: Dr Msagha J Mbogholi, PhD

Flashback from Lesson 6

- Information security policy = policy requirements (+ policy exceptions)
- There are 3 ways to document an exception: With Requirement adjustments, redress mechanisms and risk based control
- Within the infosec policy is actually a set of policies collectively making up this one document. These policies are divided into 4 distinct groups: organizational level policies, security program level policies, user security policies, and system and control policies
- The format of a standard and by extension procedure is threefold: - Policy description, description of the standard, and steps that make up the procedure.

Content

- Introduction to Cryptography
- Cryptographic Techniques
- Symmetric Encryption
- Asymmetric Encryption

Part 1

Introduction to Cryptography

Introduction

- Did you watch the epic series Game of Thrones (or GOT as it was simply known in social media circles)? If you manage to go through the first 3 episodes (yea I found those pretty boring too) the plot takes a swift turn and you will not stop watching till the last episode of the last season..8.
- How does this relate to this course…and cryptography in general?
- Well, let's find out!

Introduction (cont'd)

- The plot goes around King Robert who gets killed by a boar (I know, I know!) and then the battle for the throne begins…ah let me not spoil it any further (just watch it for yourself and enjoy the twists, turns, oohs, and ahhs…there are enough of those believe me)
- Now to the relationship with this course…In those days the nobles would exchange letters. Each letter would be written and the noble would seal it with a special seal only belonging to him/her.
- A messenger would then be given the sealed message and they would hand deliver it to the recipient noble.
- The recipient would then confirm that the letter was indeed from whom the messenger purported it to be from by examining the seal.
- It did not end there.

Introduction (cont'd)

- By confirming the source of the letter by identifying the seal, the recipient was sure of it's authenticity.
- Secondly the seal would have to be intact to confirm that the message had not been read by anybody else; this confirmed the confidentiality of the message.
- Thirdly also by confirming that the seal was intact it confirmed the integrity of the message.
- All these were confirmed by the unique seal; if the seal was not intact then it would mean the integrity, authenticity and confidentiality of the message were in question.
- Under these circumstances the messenger would pay for this with his life….yes, his life! And that is where the saying "guard this message with your life" came from.

Cryptography

- So it can be seen that from centuries ago the importance of protecting the contents of messages was well understood.
- With time the ways of doing this has changed with the dynamism and progressive nature of communication.
- In essence this is the very backbone of cryptography and defines what cryptography is all about.
- Do you remember our 3 friends from lesson 1? Bob, Ted and Tamia. Let us use them to define cryptography and its associated terms.

Cryptography (cont'd)

- Supposing Bob wishes to send a message to Tamia. He wants to ensure that nobody else reads the contents of the message. He has the option of telling Ted to "guard the message with his life" …literally; but we are past the medieval ages and this approach won't work ☺
- The other option is to find a way to convert the text using some code that only he and Tamia understand; that way anybody who somehow manages to read the message won't understand it (unless they know what the code is).
- This is the very definition of cryptography: the science (or process) of securing information over a channel such that only the intended recipient can read it.
- From cryptography comes the term cryptanalysis: this is the science (or process) of reading the coded message without (initially) knowing the code…how? We shall discuss this during this lesson.
- Further a cryptanalyst is a person who practices cryptanalysis.

Objectives of Cryptography

- At this point it is obvious that the key behind cryptography is to provide confidentiality of the message. However, this is not all; other objectives of cryptography include:
- Integrity – the recipient of the message should be able to verify that the message has not been modified (tampered with) in any way, whatsoever.
- Authentication – the recipient should be able to verify the origin (sender) of the message.
- Non-repudiation – the sender should not be able to deny sending the message, i.e. the sender can not repudiate the message.

Implementation of Objectives

- The objectives of cryptography are implemented using different techniques. Each of these techniques purposes to ensure that the message is sent and received in the exact format, with proper authentication, integrity and non-repudiation, while maintaining confidentiality. The description and workings of these techniques form the remainder of this lesson and lesson 8.
- It is also important to note that there are so many cryptographic algorithms that it is not possible to cover them all within the time and scope of this course. In this course we shall examine:
    - Symmetric encryption
    - Asymmetric encryption
    - Data Integrity algorithms

Part 2

Cryptographic Techniques

Plain Text vs Cipher Text

- When communicating between and among parties the language that is used is referred to as plain text. For example let us consider our friends Ted and Tamia.
- When Tamia wants to send a message (text) to Ted greeting him she can write something like "hello Ted." This message is written in a language both she and Ted understand namely, English. Anybody who understands English will understand what is being communicated. The same message can be written as:
- "Bonjour Ted" (French), "Habari Ted" (Kiswahili), "xin chao Ted" (Vietnamese), "salve Ted" (Latin), and so on. Thus anybody who understands any of the languages in parentheses can understand the communication.
- This form of communication (in writing) is called plain text. It means that anybody who understands the language can read and understand the communication between the two (or more parties).
- Essentially plain text can be written in any comprehensible language, not just English alone.

Plain Text vs Cipher Text (cont'd)

- Consider a situation where the parties in the communication do not want anybody to understand the communication; what are the available options?
- Ted could write to Tamia in Vietnamese or even Korean…that solves the problem temporarily, until a Vietnamese or Korean turns up ☺
- Another way he can do this is to come up with some code that only the two of them understand; did you play these games when you were younger?
- In cartoons and mystery books parties would exchange texts using a secret code that only the involved parties knew. One of the most common codes was to replace a letter with another letter further on in the alphabet. Thus if the code was to move 4 letters up the alphabet A would become E, B would become F and so on. Thus our message "hello Ted" would now become "lipps xih"; understand?

Plain Text vs Cipher Text (cont'd)

- This way the only person who can understand the message is one who knows the code! When plain text is converted to a secret message using a code it is referred to as cipher text.
- It is therefore important to understand that for it to be called cipher text a secret code must be used to convert plain text; it is not enough to just write plain text in another language (this would just remain as plain text).
- Let us try and use simple mathematics to explain the difference between the two:
  - Plain text + code = Cipher text
- Code can take any form such as the example we used of moving 4 letters up the alphabet; it could also take the form of a simple or complex algorithm as we shall see.

Cryptographic Techniques

- There are two main approaches (techniques) used to convert plain text into cipher text. These are :
- Substitution approach (techniques)
- Transposition approach (techniques)
- When they are used together it is referred to as a product cipher.

Substitution Techniques

- These techniques or approaches generally revolve around substituting plain text characters with other characters, numbers or symbols.
- They work around using an algorithm that will make the conversion from plain text to cipher text.
- The complexity of the algorithm is what makes the cipher text hard (or easy) to crack.
- There are 8 cipher techniques that use substitution approach to convert plain text into cipher text.

1. Caesar Cipher

- The Caesar cipher was first proposed by the man whom it is named after, Julius Caesar.
- The original cipher uses an algorithm that replaces each alphabetic character with another one 3 places ahead in the alphabet.
- For example, the letter A will be replaced by D, B by E, C by F, and so on.
- Your course lecturer is Dr. Msagha J Mbogholi. If we were to convert this into cipher text using Caesar cipher his name would now be GU PVDJKD M PERJKROL.
- Let us put these next to each other to see the transformation:
- DR MSAGHA J MBOGHOLI
- GU PVDJKD M PERJKROL
- Thus using the earlier formula or plain text + code = cipher text, we get:
- DR MSAGHA J MBOGHOLI + CAESAR CIPHER = GU PVDJKD M PERJKROL

2. Caesar Cipher (modified)

- As can be clearly seen the original Caesar cipher is a fairly easy one for a cryptanalyst to crack (after all it's just moving back and forth 3 steps right?)
- One way of making the cipher a bit harder to crack is to modify it such that the replacement of alphabetic characters is not necessarily 3 but any other number. Thus this means a character can move 1 or up to 25 characters (there are 26 letters in the English alphabet).
- This makes it harder for anyone to figure out what the algorithm being used is.
- Let us look at an example.

Caesar Cipher (modified)

- Suppose as a cryptanalyst you are presented with the following cipher text:
- DTZ LTY NY and you would like to crack it in order to read the original plain text message. How would you go about it?
- If it was the original Caesar cipher then it would be very easy wouldn't it?
- But now there are 25 possible replacements for each alphabetic character.
- The most practical approach in cracking this is to use brute force approach.
- A brute force approach is one whereby all possible combinations are tried in an effort to crack the algorithm.
- Applying this in our scenario produces the original plain text.

Caesar Cipher (modified)

Comb	D	T	Z	L	T	Y	N	Y
1	C	S	Y	K	S	X	M	X
2	B	R	X	J	R	W	L	W
3	A	Q	W	I	Q	V	K	V
4	Z	P	V	H	P	U	J	U
5	Y	O	U	G	O	T	I	T
6	X	N	T	F	N	S	H	S

- An application of brute force can be seen here.
- What has been done in the table is to move one letter backwards row by row so that the original plain text message can be obtained.
- Ideally all possible combinations should be tabulated but examine row 5 in the table….
- We can safely assume that we got it (see what I did there? ☺)
- This therefore shows that even this modified version isn't the best to use to create cipher text.

3. Mono-alphabetic Cipher

- As noticed from the previous example the modified Caesar cipher was fairly easy to crack since there could only be 25 possible combinations, and therefore brute force could easily be applied.
- The weakness was due to the fact that the cipher shifts all letters the same number of steps. Suppose each letter is shifted an independent number of times?
- Enter the mono-alphabetic cipher. This cipher shifts each letter independently; that is, if A is moved 3 characters to D, then B may be moved 10 characters to L, C may be moved 2 characters to E, and so on. This makes the cipher much much harder to crack!
- This means that for each character there are 26 (including itself) different combinations to explore; and in a given sentence there are millions of possible combinations to try out using brute force approach (recall the table created for the modified Caesar approach?)
- Therefore A can be anything from A to Z, B can be anything from B to A, and so on. Quite a cracker.

4. Homophonic Substitution Cipher

- There is still one weakness that can be observed from the 3 ciphers described so far; every letter is replaced by a single alphabetic letter regardless of the number of steps forward taken.
- For a seasoned cryptanalyst this makes it still not very difficult to crack as long as s/he has good command of English. There are certain words in a sentence that can be guessed, especially two (and some three) letter words.
- These words can be 'for', 'if', 'to', 'you', 'we', 'so', 'and', and so on. Further there are certain letters that have a higher probability of appearing in a sentence than others.
- It is therefore still possible to crack a mono-alphabetic cipher.

Homophonic Substitution Cipher

- The homophonic substitution cipher makes it that much more difficult for a cryptanalyst to crack.
- It works by substituting each alphabetic letter with a series of other alphabetic letters, not just one.
- Thus J can be L, T, V, X, Z while D might be G, K, N, O.
- Mathematically this would mean J → {L, T,V,X,Z} and D → {G, K, N, O}
- This makes the cipher extremely difficult to crack as the cipher can pick any of the letters for substitution in different instances where the same letter is used.

5. Polygram Substitution Cipher

- This cipher substitutes blocks of characters rather than individual characters.
- The blocks of characters are never the same even for words which may have a repeating sequence in them.
- For example the cipher for ‘FOR’, ‘FORE’, ‘FORMER’, ‘FORD’ will all be different despite the block ‘FOR’ being repeated in all of them.
- FOR → XYZ, FORE → ABCD, FORD → JKSU and so on.

6. Polyalphabetic Substitution Cipher

- The key behind all substitution ciphers is to substitute a character with another; the complexity is in determining which character has replaced which one.
- Polyalphabetic substitution uses several one-character keys to replace the individual alphabetic characters using the keys….makes sense?
- Ok, a good example is a well known polyalphabetic cipher known as Vigenére cipher. This cipher uses a table which references each character using a key. Each of the plain text characters is replaced with an instance of the given key; thus 1st instance is replaced with 1st instance of the key, 2nd is replaced with 2nd instance of the key, and so on.
- The cipher utilizes the Vigenére tableau; a good application of this can be found in Stallings (2011, pg 49-50)

Other Substitution Ciphers

- Due to time and space limitations a comprehensive discussion on all substitution ciphers is not possible. However, two other substitution ciphers worth mentioning that the reader can do more reading on are:
- Playfair cipher
- Hill Cipher

Transposition Techniques

- Transposition techniques are adapted from the English word to ‘transpose’.
- This means to exchange or cause things to exchange.
- These techniques work by exchanging characters using some kind of operation depending on the algorithm used. In technical terms they perform some kind of permutation on the text.
- They are different from substitution techniques as they don’t perform any substitution of characters.

1. Rail-fence Technique

- This is a simple transposition algorithm that takes a string, reads it diagonally, and outputs it as a single row. Let us demonstrate this using an example to make it easier to understand.
- Suppose we have the string " Maths is easy"
- Reading it diagonally produces
- M t s s a y
- a h i e s

Next the diagonal string is read horizontally producing the cipher text 'mtssayahies'

2. Columnar Transposition (Basic)

- What are your thoughts on the rail-fence technique? Can it be cracked using brute force approach? Of course! A determined cryptanalyst can since it is not a very complicated approach.
- Another way of creating cipher text is using a columnar transposition approach.
- In the most basic form the words making up the string are arranged in a table in a row by row manner and then output in a columnar output. The output doesn't have to follow the order of columns.
- Let us demonstrate this using our previous example string " Maths is easy"
- In this example we shall make use of a 4 column table

Columnar Transposition (Basic)

Column 1	Column 2	Column 3	Column 4
m	a	t	h
s	i	s	e
a	s	y	

- The output does not have to follow the order of the columns (this would make it easier for a cryptanalyst to crack).
- An appropriate way to output is to use a random and not sequential output order of columns.
- In this case let us output in the order of column 3, column 1, column 2, column 4
- This produces our cipher text as 'tsymsaaishe'

3. Columnar Transposition (Multiple)

- This technique uses the same basic columnar transposition technique.
- The difference is that the table is used multiple times to make the cipher text harder to crack.
- The first output is similar to the basic transposition technique.
- The cipher text output is then re-introduced to the same table and then output again…this process is repeated a number of times.
- Let us do this one time using the cipher text generated using the basic columnar transposition approach.

Columnar Transposition (Multiple)

- From the first round of transposition the cipher text produced was 'tsymsaaishe'. This cipher is now passed to the table a second time:

Column 1	Column 2	Column 3	Column 4
t	s	y	m
s	a	a	i
s	h	e	

- Using the same approach as before we output the columns in the following order: 3, 1, 2, 4
- This gives the new cipher as yaetsssahmi.
- The process can be repeated as many times as deemed necessary.

4. Vernam Cipher

- This cipher uses a one time key for each plain text message to create a cipher text message.
- The one –time key is randomly generated from a one-time pad and is only used once in any given sequence of conversion. After it is used it is discarded.
- Let us use our string ‘maths is easy’ to demonstrate how this cipher works.
- Each letter of the alphabet is treated as a number starting from 1, that is A = 1, B=2, C=3, ….Z=26.
- Take each character of the input string and add it to the one-time key and obtain the totals. For those above 26 subtract 26 from the total in order to obtain a number less than 26.
- The length of the one-time key must be equal in length to the plain text that will undergo conversion.
- In this case the length of our string is 11 characters => the one-time key string will have 11 characters as well, say ‘asdfghjklqe’

Vernam Cipher

- Next the one-time key is added to the string as follows:

Plain	m	a	t	h	s	i	s	e	a	s	y
Value	13	1	20	8	19	9	19	5	1	19	25
One Time key	a	s	d	f	g	h	j	k	l	q	E
Value	1	19	4	6	7	8	10	11	12	17	5
Sum	14	20	24	14	26	17	29	16	13	36	30
Subtract 26 from values above 26	14	20	24	14	26	17	3	16	13	10	4
Cipher text	n	t	x	n	z	q	c	p	m	j	d

Vernam Cipher

- Notice that no 2 letters in the original plain text that are the same character are also the same in cipher text.
- Further no 2 similar letters in cipher text, for example ‘n’ which appears twice, represent the same character.
- Lastly since the one-time key is only used once then it is that much harder to decipher.
- This is why this cipher has been described as the perfect cipher in many security circles.

Part 3

Symmetric Encryption

Encryption & Decryption

- In part 2 we have examined different ways by which plain text can be converted into cipher text using various cryptographic techniques.
- In cryptography the process of converting plain text into cipher text is referred to as encryption. Another term used for cipher text is encrypted text.
- Thus by encrypting text one is able to protect the CIA of the plain text (remember the objectives of cryptography discussed earlier in this lesson?)
- The algorithms that are used to encrypt plain text are referred to as encryption algorithms; conversely the algorithms used to convert cipher text back to plain text are referred to as decryption algorithms.
- Further in encryption different types of keys are used: a key is used on the algorithm in order to convert the plain text into cipher text., this is to say
- Plain text + (key)Encryption algorithm = cipher text.

Encryption and Decryption

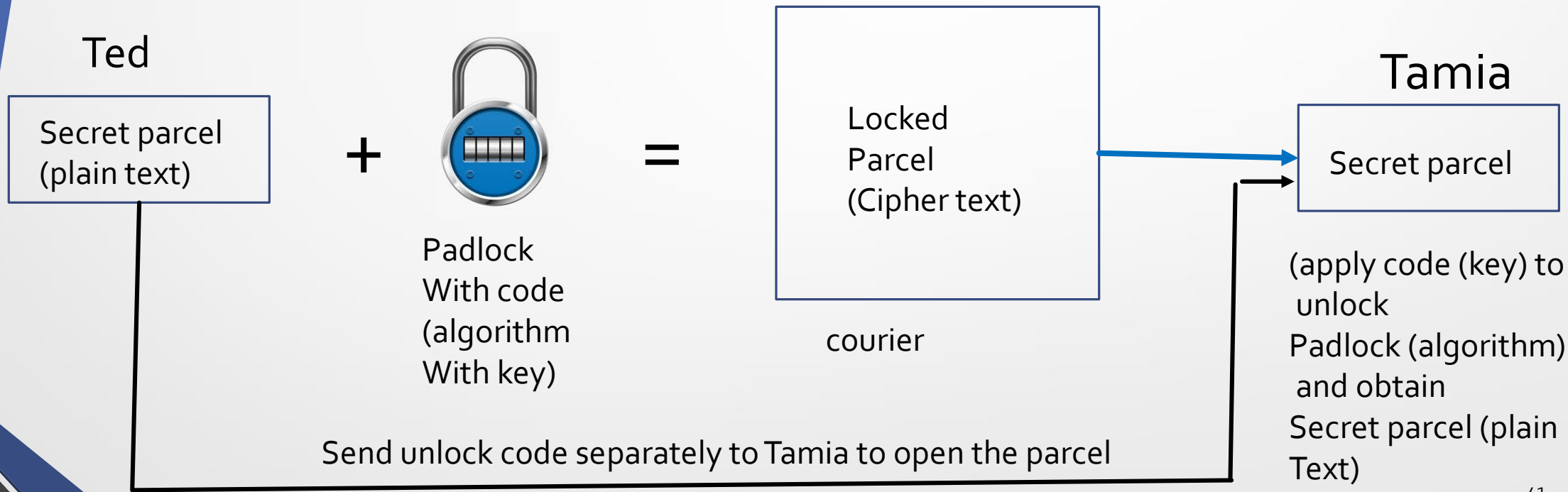
- Therefore,
- plain text + encryption algorithm = cipher text; and cipher text + decryption algorithm = plain text
- In principle and also as is to be expected, the encryption and decryption algorithm have to be the same (the same method is used to encrypt and decrypt).
- Mathematically the decryption algorithm is the inverse of the encryption algorithm and vice versa.
- That is to say, if the encryption algorithm is E , then the decryption algorithm will be $(E)^{-1}$
- In an information channel the data needs to be protected using different means so that its CIA is maintained; further it is desirable that the property of non-repudiation is maintained.
- Two ways of encryption are generally used.
- These are symmetric encryption and asymmetric encryption.

Symmetric Encryption

- Recall our friends Ted and Tamia? Let us use them to describe symmetric encryption simply.
- If Ted wishes to send a secret parcel to Tamia then he can use a courier and lock the message in a box using a padlock. This will ensure that neither the courier nor anyone else can access the secret contents of the parcel. The challenge is in how Tamia will open the box! There are different types of padlocks and all are opened using a key.
- The key might be physical or a code that is input and opens the padlock.
- If it is a code then Ted has to find a separate way to get the code to Tamia so that she can open the box. If it is a physical key then it is that much harder.
- One way of sending the code in today's day and age is through an electronic message (email or text sms); but then again how safe is it?
- We can look at the padlock as the algorithm in symmetric encryption and the code as the encryption key.

Symmetric Encryption

- Tamia (or anyone else for that matter) might be able to identify the type of padlock (algorithm) used to lock (encrypt) the message. However, she can only access the contents using the code (encryption key).
- In symmetric key encryption the same key that is used to encrypt a message is the same one that is used to decrypt it. This is to say that it is **a shared key**. It can be demonstrated as follows



Applications of Symmetric Encryption

- There are several applications of symmetric encryption and the common ones are mentioned briefly here. References at the end of this lesson should be used to further understand the specific applications:
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- Blowfish
- RC 4/5
- Other block and stream ciphers.

Asymmetric Encryption

- Asymmetric encryption (also known as public key encryption) purposes to make the process more secure.
- In asymmetric encryption the key that is used to encrypt the plain text is different from the key that is used to decrypt the cipher text.
- This introduces two key terms associated with asymmetric encryption and these are private and public keys.
- What keys do has already been discussed; however, in symmetric key encryption the process was simple as the key used to lock (encrypt) the message is the same one that is used to unlock (decrypt) it.

Asymmetric Encryption

- Whenever a user accesses the Internet a public key is immediately created for them (yes even you who is reading these notes).
- The public key is available and can be accessed from anywhere as soon as the user connects to the Internet.
- Additionally every user has a private key; this belongs to an individual and can only be used by them.
- These keys are in the form of a string that uniquely identifies the individual; they are issued by certification authorities online.
- Thus every user has the pair of keys (public and private) that uniquely identifies them online.

Asymmetric Encryption

- The principle behind asymmetric encryption is to take advantage of the fact that an individual's public key is widely disseminated, while their private key is unique to them.
- Since the pair of keys is generated by a trusted third party (a certification authority) then users can be assured that their private keys can not be accessed by intruders or any other third party for that matter.
- Asymmetric encryption works by having the sender encrypt the message using the recipient's public key (widely available) and then having the recipient decrypt the message using their own private key (which only belongs to them).
- Since the keys are in pairs a user's private key is the only one that can unlock messages that have been locked with their public keys.
- Let us demonstrate this using a diagram

Asymmetric Encryption

- Asymmetric encryption demonstrated.

Step 1 (sender)

Ted's plain text message

+

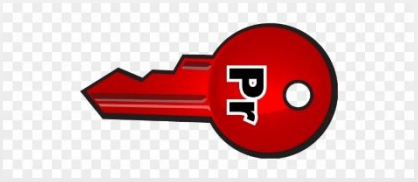
Tamia's public Key

=

Cipher text

Step 2 (recipient)

+



Tamia's private key

=

Ted's plain text message

Applications of Asymmetric Encryption

- There are several applications of asymmetric encryption and the common ones are mentioned briefly here. References at the end of this lesson should be used to further understand the specific applications:
- Diffie – Hellman Key Exchange
- RSA
- ElGamal
- Rabin

Summary

- Cryptography is the science (or process) of securing information over a channel such that only the intended recipient can read it.
- Messages that are written in human comprehensible language are called plain text, while a message that has been changed according to some rules is called cipher text.
- Cryptographic techniques include the substitution and transposition ciphers approach.
- In symmetric encryption a shared key is used to both lock and unlock a message (text). Examples of application of symmetric encryption are DES, RC4/5, Blowfish and AES.
- In asymmetric encryption a different key is used to lock and unlock a message (text). Examples of application of asymmetric encryption are Diffie-Hellman, RSA, Rabin and ElGammal.

References

- Delfs, H., & Knebl, H. (2007). *Introduction to cryptography: Principles and applications*. Springer.
- Kahate, A. (2013). *Cryptography and network security*. McGraw Hill Education.
- Stallings, W. (2011). *Cryptography and network security: Principles and practice*. essay, Prentice Hall.