DCIT 111 (INTEGRATED PROGRAMMING AND TECHNOLOGIES 2) MIDTERMS REVIEWER

LESSON 1: Cipher Cryptography

Scripting Language vs Programming Language

FACTOR	SCRIPTING LANGUAGE	PROGRAMMING LANGUAGE
Type of language	Interpreter based	Compiler based
Usage	To combine existing components	To develop from scratch
Running	Inside other program (dependent)	Independent of a parent program
Conversion	High level instructions converted to machine language	Full program converted to machine language in one time
Design	Makes coding simple and fast	Gives full use of language
Compilation	No need to compile	Needs to compile first
File type	Does not create a file type	Creates a .exe file
Coding type	It is a small piece of code	It is a full code of a program
Time to develop	Less time as required less code	More time as you need to write the full code
Complexity	Easy to write and use	Difficult
Interpretation	It is interpreted in another program	Stand-alone compile result, no need to be interpreted by another program
Length	Only a few and short lines of coding	Numerous lines for every function
Hosting requirement	Requires a host	Self-executable, no host needed
Support	Limited or no support to user interface design, data types, and graphic design	Rich support to user interface design, data types, and graphic design
Cost	Low maintenance	High maintenance
Example	JavaScript, PHP, Ruby, Perl, VB Script, etc.	C, C++, Java, Pascal, C#, VB, Basic, COBOL, etc.

Cryptography

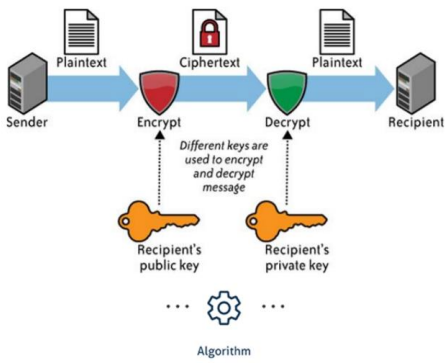
- the process of communicating secretly through the use of ***ciphers***, and ***cryptanalysis***, the process of cracking or deciphering such secret communications.

– a method of protecting communication and information through the use of codes so that only those who are meant to receive the information can read and process it.

– a set of calculations called algorithms that transform hard to decipher messages: cryptographic key generating, digital signatures, and verifications.

ENCRYPTION AND DECRYPTION PROCESS

- Procedure
- Conversion
- Algorithm
- Techniques



TECHNIQUES

Cryptology - defined as the study of cryptography or cryptanalysis.

Cryptology and cryptanalysis

- are the disciplines that relate to cryptography and techniques like microdots and image-word merging help hide information in transit or storage.

- Confidentiality
- Integrity
- Non-repudiation
- Authentication

Cryptosystem - include the regulation of human behaviors like choosing complicated passwords and logging off unused systems.

Cryptographic algorithm

- set of procedures that encrypt or decrypt messages to secure computer system communications within devices such as smartphones as well as applications.

Types:

Symmetric Cryptography

Asymmetric Cryptography

Hybrid Cryptography

Symmetric Cryptography Algorithm

Symmetric Key Cryptography

1. Plaintext - is the original data / message that the algorithm uses as input.

2. Encryption Algorithm - The encryption algorithm performs various mathematical operations on this plaintext data to encrypt it.

3. Ciphertext - This is the scrambled message that is the result of the encryption algorithm. If intercepted by an untrusted user, it is merely seen as garbled data.

4. Secret key – also input to the encryption algorithm. The encrypted data / message is then sent to the end user, who uses the same secret key to decipher the data.

5. Decryption Algorithm - It takes the ciphertext, the secret key, and produces the original data / message. In

simple words, it runs the encryption algorithm in reverse sequence.

Symmetric Ciphers – cryptosystems that use the same key to encrypt and decrypt messages.

Types:

Block cipher operates on blocks of a fixed size, usually 64 or 128 bits.

• Blowfish • DES • AES (Rijndael)

Stream ciphers generate a stream of pseudo-random bits, usually either one bit or byte at a time.

• Keystream • XORed

Block Cipher

Confusion – refers to methods used to hide relationships between the plaintext, the ciphertext, and the key.

Diffusion - serves to spread the influence of the plaintext bits and the key bits over as much of the ciphertext as possible.

DES uses a Feistel network – used in many block ciphers to ensure that the algorithm is invertible

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

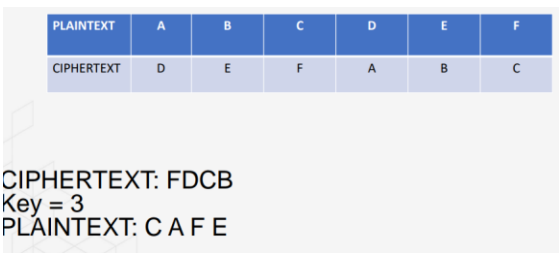
Data Encryption System(DES) Encryption Algorithm

– Algorithms create a fixed length of block ciphers with a secret key that the sender uses to encipher data and the receiver uses to decipher data

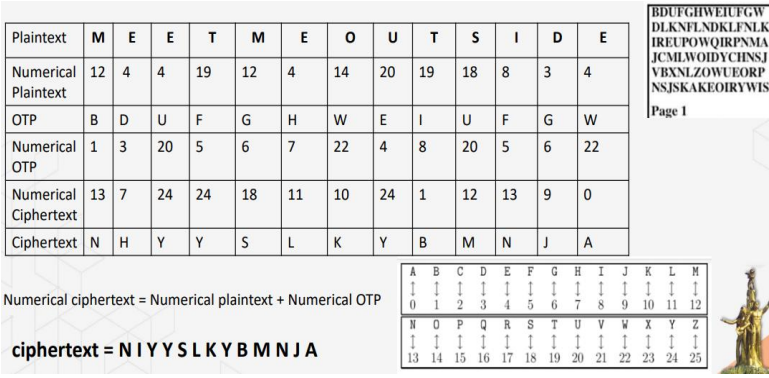
Advanced Encryption Standard (AES) Encryption Algorithm

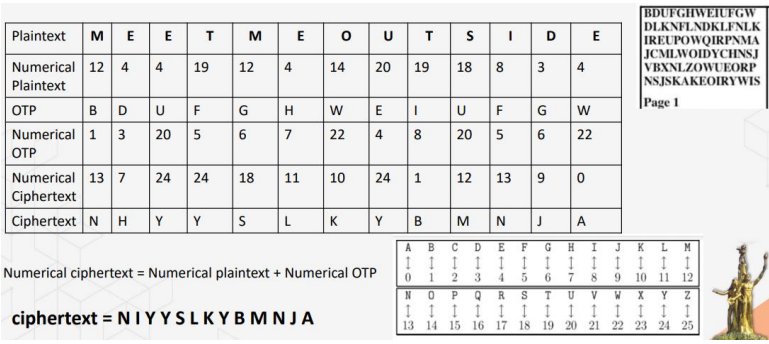
– the Rijndail algorithm that is capable of 256-bit (or more) key to prevent hacker intrusions: Wireless security, Processor security and file encryption, SSL/TLS protocol (website security), Wi-Fi security, Mobile app encryption, VPN (virtual private network), etc

Block Cipher



Stream Cipher (OTP)





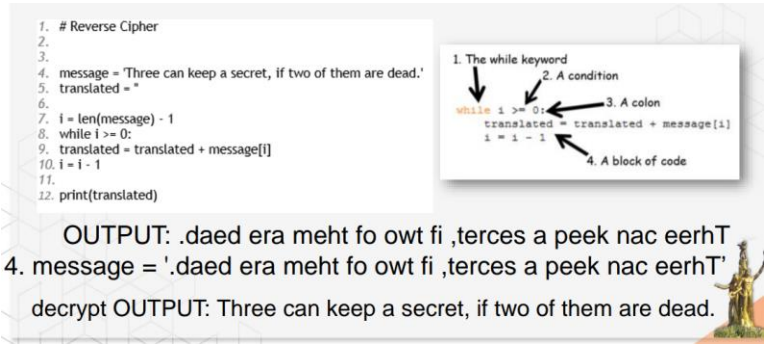
TECHNIQUES:

Cipher – method in which a message is transformed to conceal its real meaning.

Cipher algorithm - protocol embedded process involves private and public key generation for data encryption/decryption, digital signing, and verification for message authentication.

Reverse Cipher

Reverse cipher - encrypts a message by printing it in reverse order.



LESSON 2: SOFTWARE SECURITY PRACTICES

Evidence-based Security vs Code Access Security

Evidence-Based Security

– controls applications

- access rights based on who wrote the code, what the code is trying to do, where it was installed from, and who is trying to turn it.

Advantages:

✓ Management can be restricted to using only well-defined interfaces.

✓ Code can be downloadable from unsecured sources and safely executed

✓ Applications composed of many components can be safely installed with multiple security levels

Code Access Security

- protect the system from code that may be malicious or just Unstable

- automatically installed with .NET Framework and with Visual Studio.

Security Levels

▪ Enterprise Policy

▪ Machine Policy

▪ User Policy

▪ Application Domain Policy

Machine Policy

▪ Defined by machine administrators who set policy for one computer

▪ Can set policy that excludes modification from the user level but not from the enterprise level

Enterprise Policy

▪ Defined by enterprise administrators who set policy for enterprise domains

▪ Affects every computer and user on the network

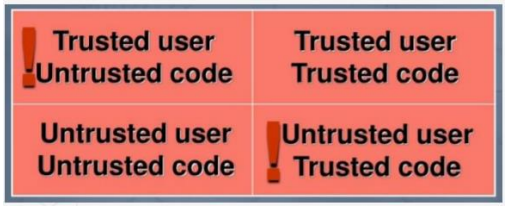
▪ Evaluated at the runtime

User Policy

▪ Lowest administrable policy level

▪ Defined by users who set policy for a single logon account

▪ This level is configurable by the current logged-on user



Application Domain Policy

▪ Defined by the runtime host for setting load-time policy

▪ Cannot be administered

Authentication to system resources and services

✓ **Role-Based Security** – enforces security permissions based on user identity by implementing the following concepts:

Authentication – Examines user, or a principal identify through username and password verifications

Authorization – Enables or restricts principal access to specific applications/role

✓ **Web Application Security**

Additional Authentication – Authentication protocols like cookie, etc.

Additional Authorization – URL authorization allows or denies access to URLs based on user identity or roles

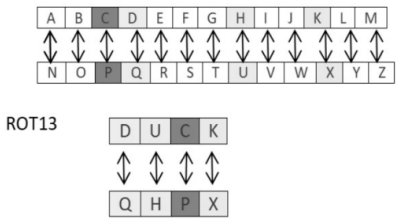
Classic Encryption Methods

The Caesar Cipher - an ancient trick where you just move every letter forward characters in the alphabet based on the key

Example:
Plaintext : B I L Z
Key: 4
Ciphertext : F M P D

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

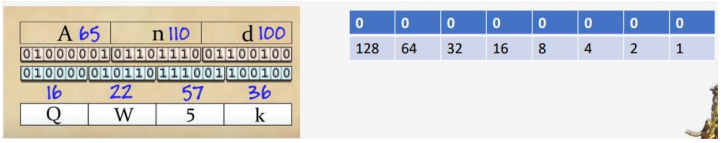
ROT13 Algorithm - refers to the abbreviated form Rotate by 13 places. It is a special case of Caesar Cipher in which shift is always 13. Every letter is shifted by 13 places to encrypt or decrypt the message.



Base64 Encoding

- term Base64 originates from a specific MIME content transfer encoding.

- commonly used when there is a need to encode binary data that needs to be stored and transferred over media that are designed to deal with ASCII



XOR Cipher Algorithm

XOR algorithm of encryption and decryption

- converts the plain text in the format ASCII bytes

- uses XOR procedure to convert it to a specified byte.

It offers the following advantages to its users:

✓ Fast computation

✓ No difference marked in left and right side

✓ Easy to understand and analyze

Bit 1	Operation	Bit 2	Result
0	⊕	0	0
1	⊕	0	1
0	⊕	0	1
1	⊕	1	0

Encryption			
Text	S	u	n
ASCII Code	83	117	110
Binary	01010011	01110101	01101110
Key	01010010	01010010	01010010
Cipher	00000001	00100111	00111100

XOR Encryption

Encryption			
Cipher	00000001	00100111	00111100
Key	01010010	01010010	01010010
Output	01010011	01110101	01101110
ASCII Code	83	117	110
Text	S	u	n

LESSON 3: BRUTE-FORCE TECHNIQUE

Attack Models

-a set of assumptions about how attackers might interact with a cipher and what they can and can't do.

Goals:

• To set requirements for cryptographers who design ciphers, so that they know what attackers and what kinds of attacks to protect against.

• To give guidelines to users, about whether a cipher will be safe to use in their environment.

• To provide clues for cryptanalysts who attempt to break ciphers, so they know whether a given attack is valid.

Black-Box Models

– controls applications

- access rights based on who wrote the code, what the code is trying to do, where it was installed from, and who is trying to turn it.

Advantages:

✓ Management can be restricted to using only well-defined interfaces.

✓ Code can be downloadable from unsecured sources and safely executed

✓Applications composed of many components can be safely installed with multiple security levels

Different Black-box attack models:

1. Ciphertext-only attackers (COA) observe ciphertexts but don't know the associated plaintexts, and don't know how the plaintexts were selected.

2. Known-plaintext attackers (KPA) observe ciphertext and plaintext and do know the associated secret key.

3. Chosen-plaintext attackers (CPA) can perform encryption queries for plaintexts of their choice and observe the resulting ciphertexts.

Gray-Box Models

♣ the attacker has access to a cipher's implementation.

♣ This makes gray-box models more realistic than black-box models for applications.

♣ depend on physical, analog properties rather than just on an algorithm's input and outputs, and crypto theory will often fail to abstract the complexity of the real world

Models of Gray-Box Models

1. Side-channel attacks

• a family of attacks within gray-box models.

• a source of information that depends on the implementation of the cipher, be it in software or hardware.

• Side-channel attackers observe or measure analog characteristics of a cipher's implementation but don't alter its integrity; they are noninvasive.

2. Invasive attacks

♣ a family of attacks on cipher implementations that are more powerful than side-channel attacks, and more expensive because they require sophisticated equipment

♣ consist of a whole set of techniques and procedures, from using nitric acid to remove a chip's packaging to microscopic imagery acquisition, partial reverse engineering, and possible modification of the chip's behavior with something like laser fault injection.

White Box Models

♣ Attacks with full privilege have complete access to the implementation algorithms.

♣ Dynamic execution can be observed and important data such as cryptographic keys can be seen.

♣ Detailed algorithms in the system are completely visible and alterable.

Security Goals for an Attacker:

1. Semantic Security and Randomized Encryption: IND-CPA

• The most important security notion is IND-CPA, also called semantic security. It captures the intuition that ciphertexts shouldn't leak any information about plaintexts as long as the key is secret.

o encryption must return different ciphertexts if called twice on the same plaintext; otherwise, an attacker could identify duplicate plaintexts from their ciphertexts, contradicting the definition that ciphertexts shouldn't reveal any information.

o uses randomized encryption. It randomizes the encryption process and returns different ciphertexts when the same plaintext is encrypted twice.

2. Achieving Semantically Secure Encryption

• deterministic random bit generator (DRBG) – an algorithm that returns random-looking bits given some secret value.

3. Comparing Security Notions

• IND-CCA implies IND-CPA

• NM-CCA implies NM-CPA

3 Types of Encryption Applications (Security)

1. **In-transit encryption** protects data sent from one machine to another: data is encrypted before being sent and decrypted after being received, as in encrypted connections to ecommerce websites.

2. **At-rest encryption** protects data stored on an information system. Data is encrypted before being written to memory and decrypted before being read.

3. **Encryption in use:** protects your data in memory from compromise or data exfiltration by encrypting data while being processed. For more information

Categories of Breaking an Algorithm (Lars Knudsen)

1. **Total break**. A cryptanalyst finds the key.

2. **Global deduction.** A cryptanalyst finds an alternate algorithm

3. **Instance (or local) deduction**. A cryptanalyst finds the plaintext of an intercepted ciphertext.

4. **Information deduction**. A cryptanalyst gains some information about the key or plaintext.

Unconditional Security

A cryptographic system is considered to be **unconditionally secure**, sometimes called strong, if it cannot be broken, even with infinite computational resources. This implies that cryptanalysis is impossible and that even if every possible key were tried in an exhaustive brute-force attack, it would be impossible to determine which key was the correct one.

brute-force attack

Brute Force

• The phrase **brute force** means the illegal effort of breaking into the back end of a system to get the username/password combination. It could consist of trial-and-error methods; it could be a planned effort, with well structured, automated attacks using bots.

• **brute-force attack** - The technique of trying every possible decryption key

---

LESSON 4: ENCRYPTING & DECRYPTING WITH THE TRANSPOSITION CIPHER

Transposition Ciphers

Transposition cipher technique - the plaintext remains the same, there is no text replacement of alphabets or numbers occurs but the order of characters are changes or reorder to produce to cipher

- Although many modern algorithms use transposition, it is troublesome because sometimes it requires messages to be only certain lengths.

Types of Transposition Ciphers

1. Rail Fence Transposition

2. Book Cipher/Running Key Cipher

3. Improved Columnar Transposition

4. Columnar Transposition

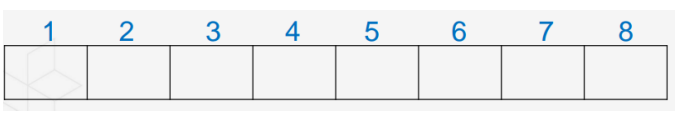
- form of transposition cipher in which plain text represent in matrix form.

- involves writing the plaintext out in rows and then reading the cipher text off in columns one by one.

Encryption Process:

1. Count the number of characters in the message and the key. Example: Love is not blind. 18 characters

2. Draw a row of a number of boxes equal to the Key. Key = 8



3. Start filling in the boxes from left to right, entering one character per box.

1	2	3	4	5	6	7	8
L	o	v	e	_	i	s	_

4. When you run out of boxes but still have more characters, add another row of boxes.

1	2	3	4	5	6	7	8
L	o	v	e	_	i	s	_
n	o	t	_	b	l	i	n
d	.						

5. When the last character is reach, shade in the unused boxes in the last row.

1	2	3	4	5	6	7	8
L	o	v	e	_	i	s	_
n	o	t	_	b	l	i	n
d	.						

6. Starting from the top left and going down each column, write out the characters. When you get to the bottom of a column, move to the next column to the right. Skip any shaded boxes.

1	2	3	4	5	6	7	8
L	o	v	e	_	i	s	_
n	o	t	_	b	l	i	n
d	.						

ENCRYPTED MESSAGE: Lndoo.vte__bilsi_n

Decryption Process:

ENCRYPTED MESSAGE: Lndoo.vte__bilsi_n
Key= 8

1. Calculate the number of columns you need by dividing the length of the message by the key and then rounding up.
Cipher text length: 18 characters
18 / 8 = 2.25 = 3

1	2	3

2. Draw boxes in columns and rows. Use the number of columns calculated in step 1. The number of rows is the same as the key.

	1	2	3
1			
2			
3			
4			
5			
6			
7			
8			

3. Calculate the number of boxes to shade in by taking the total number of boxes (the number of rows multiplied by the number of columns) and subtracting the length of the cipher text message.

4. Shade in the number of boxes you calculated in step 3 at the bottom of the rightmost column.

	1	2	3
1			
2			
3			
4			
5			
6			
7			
8			

5. Fill in the characters of the cipher text starting at the top row and going from left to right. Skip any of the shaded boxes.

	1	2	3
1	L	n	s
2	o	o	.
3	v	t	
4	e	_	
5	_	b	
6	i	l	
7	s	i	
8	_	n	

6. Get the plaintext by reading the leftmost column from top to bottom, and continuing to do the same in each column.

PLAINTEXT:
Love is not blind.

	1	2	3
1	L	n	d
2	o	o	.
3	v	t	
4	e	_	
5	_	b	
6	i	l	
7	s	i	
8	_	n	