Classical Ciphers

CS 363 Computer Security

Review

A(n) _____ is an attempt to learn or make use of information from the system that does not affect system resources.

A passive attack

B inside attack

C outside attack

D active attack

Review

An example of _____ is an attempt by an unauthorized user to gain access to a system by posing as an authorized user.

A interception

B masquerade

C inference

D repudiation

Review

A _____ provides distribution channels, such as an online shop or a Web retailer.

A content provider

B consumer

C clearinghouse

D distributor

Review

A _____ is a word, name, symbol, or device that is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others.

A copyright

B patent

C trademark

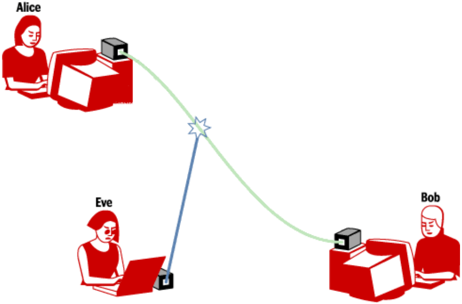
D all of the above

Definitions

Cryptology consists of

- *cryptography* - study of ways of keeping information secure.
- *cryptanalysis* - analysis of cryptographic algorithms and procedures to find weaknesses.

Cryptographers design algorithms that Alice and Bob can use to exchange information so that Eve can't read it. Cryptanalysts like Eve try to access encrypted information without knowing the encryption algorithm or key.



More Definitions

- The Greek word *kryptos* means “hidden” or “covered” and the Arabic word *sifr* is the root of the English word *cipher*.
- A *code* exchanges characters or words or phrases for different ones. Encoding a message is not necessarily for the purpose of concealment.
- *Encrypting (decrypting)* and *enciphering (deciphering)* are synonymous.
- The original message is *plaintext* and the hidden message is *ciphertext*.

Famous Codes - Morse Code

Morse code in the 1830s for the telegraph by Samuel B. Morse, who was an art professor at NYU. His first message[1] was

· — —   · · · ·   · —   —   · · · ·   · —   —   · · · ·   — — ·   — — —   — · ·

· — —   · — ·   — — —   · · —   — — ·   · · · ·   —

A	· —	N	— ·	0	— — — — —
B	— · · ·	O	— — —	1	· — — — —
C	— · — ·	P	· — — ·	2	· · — — —
D	— · ·	Q	— — · —	3	· · · — —
E	·	R	· — ·	4	· · · · —
F	· · — ·	S	· · ·	5	· · · · ·
G	— — ·	T	—	6	— · · · ·
H	· · · ·	U	· · —	7	— — · · ·
I	· ·	V	· · · —	8	— — — · ·
J	· — — —	W	· — —	9	— — — — ·
K	— · —	X	— · · —	Fullstop	· — · — · —
L	· — · ·	Y	— · — —	Comma	— — · · — —
M	— —	Z	— — · ·	Query	· · — — · ·

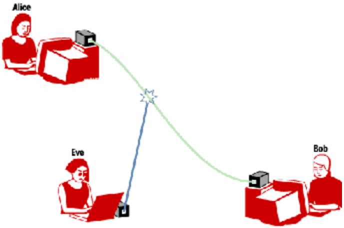
Why do letters E, I, and T have the shortest codes and J, Q, X, Y, and Z have the longest codes?

[1] Numbers 23:23

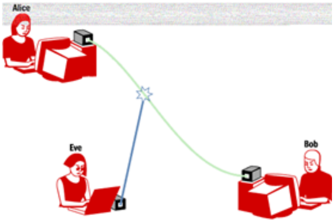
Steganography

Steganography (meaning “covered writing”) hides the very existence of messages. The messages may be easy to read if found.

Can you see MasterCard hidden in either image?



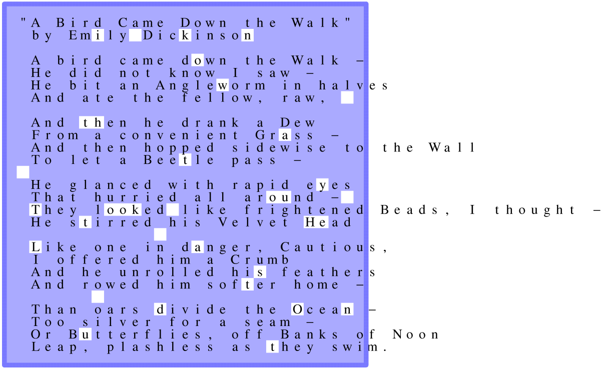
Least significant bit



6 least significant bits

Stencils

Stencils can be used to conceal messages in regular texts. These were used by the ancient Chinese and were reinvented 500 years ago by Girolamo Cardano. Such stencils are sometimes called Cardan grilles.



"A Bird Came Down the Walk"
by Emily Dickinson

A bird came down the Walk –
He did not know I saw –
He bit an Angleworm in halves
And ate the fellow, raw,

And then he drank a Dew
From a convenient Grass –
And then hopped sidewise to the Wall
To let a Beetle pass –

He glanced with rapid eyes
That hurried all around –
They looked like frightened Beads, I thought –
He stirred his Velvet Head

Like one in danger, Cautious,
I offered him a Crumb
And he unrolled his feathers
And rowed him softer home –

Than oars divide the Ocean –
Too silver for a seam –
Or Butterflies, off Banks of Noon
Leap, plashless as they swim.

Classical ciphers

Classical ciphers are often divided into transposition ciphers and substitution ciphers.

- substitution cipher: letters (or groups of letters) are systematically replaced throughout the message for other letters (or groups of letters).
- transposition cipher: letters themselves are kept unchanged, but their order within the message is scrambled according to some well-defined scheme.

Easy Cryptogram

Cryptograms are simple substitution ciphers that are popular puzzles. Let's solve this one.

```
UBPCH: XHBP NBZ BN, OUCHC EHC OUHCC ZESK OB GB OUFNVK: OUC
    HFVUO ZES, OUC ZHBNV ZES, ENG OUC PEY ABZCH ZES.
QEHO: FKN'O OUEO LRKO OUC ZHBNV ZES?
UBPCH: SCEU, QRO XEKOCH!
```

Letter Frequencies

A	B	C	E	F	G	H	K	L	N	O	P	Q	R	S	U	V	X	Y	Z
1	10	14	12	3	2	12	5	1	7	16	4	2	2	6	12	4	2	1	9

Difficult Cryptogram

This cryptogram is daunting without the spacing and punctuation.

```
GKVLKUFFWAWLSPCHPQPNZWRHZKJAWYZSHOKWZHFZHKFRKPUAOPWUHQPNZWRHZ
KJAWYZSHGJFZWZHDDHGFZWKJHFZSPZAWUZRWPUNQSHKHDJIHZSHZJGHQHQHUZ
WCHKZWFSHDVNCJDDHALKJURZSHQPKJQWKHPUWUJWUWUGNVHDZQSJXSQPFZSHF
ZNDHPZZSHZJGHNWLXWLDAUZRHZZSWFHQSJZHWUHFNWLXWLDAWUDNRHZZSWFHV
JRNHDDWQWUHFUWQQSHKHQPFJWSNHPSZSHJGOWKZPUZZSJURQPFJQPFQHPKJUR
PUWUJWUWUGNUHDZQSJXSQPFZSHFZNDHPZZSHZJGHNWLXWLDAUZRHZZSWFH
```

Anagrams

Anagrams are simple transposition ciphers that are also popular puzzles.

```
YVAN EHT NIOJ
```

The combination of substitution and transposition can provide a formidable encryption algorithm.

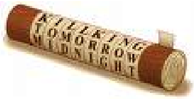
Punctuation is (usually) a Luxury

Punctuation makes text easier to read, but `ITISNOTREALLYNECESSARYYOUCANSTILLREADTHISEVENTHOUGHITISIWRITTENINALLCAPSWITHNOPUNCTUATION`

`What does MANEATINGSNAKE mean?`

`FYWNTRLCHLLNGTRTHSWTHTNVWLS`

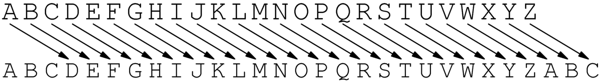
Spartan Scytale



The ancient Spartans used the $\sigma\kappa\upsilon\tau\acute{\alpha}\lambda\eta$ for encryption on the battlefield. This is an example of a transposition cipher since the letters of the message are scrambled but not changed.

The Caesar Cipher

Julius Caesar reportedly used a simple substitution scheme he used in which every letter is shifted forward 3 places.



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

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 A B C

For example “Veni, vidi, vici”[2] is enciphered as

`YHQLYLGLYLFL.`

[2] This was Caesar’s famous report to Rome in 47 B.C. after his overwhelming defeat of King Pharnaces II of Pontus at the battle of Zela.

Security of the Caesar Cipher

- Intercepted messages are easily decrypted as long as the adversary knows Caesar's algorithm, so it really offers no security.
- The Caesar cipher can be strengthened by sender and receiver agreeing in advance on a shift of anywhere from 1 to 25 letters. The amount of the shift is called the *key*.
- This might provide sufficient security for tactical situations on the battlefield, but would not provide long-term security because adversaries could simply exhaust all possible values for the key until they find the right one.

Security of the (modified) Caesar Cipher (continued)

Suppose you intercept the message “AOYSOBSKDZOBGHOB” and you know it was encrypted with a shift cipher. You could just try every possibility until you find the proper shift.

Shift	Putative Plaintext
1	znxrnarjcynafgna
2	ymwqmzqibxmzefmz
3	xlvplyphawlydely
4	wkuokxogzvkxcdkx
5	vjtnjwnfyujwbcjw
6	uismivmextivabiv
7	thrlhuldwshuzahu
8	sgqkgtkcvrgtyzgt
9	rfpjfsjbuqfsxyfs
10	qeoieriatperwxer
11	pdnhdqhzsodqvwdq
12	ocmgcpgyrncpuvcp
13	nblfbofxqmbotubo
14	makeanewplanstan
15	lzjdzmdvokzmrszm
16	kyicylcunjylqryl
17	jxhbxkbtmixkpqxk
18	iwgawjaslhwjopwj
19	hvfzvizrkgvinovi
20	gueyuhyqjfuhmnuh
21	ftdxtgxpietglmtg
22	escwsfwohdsfklsf
23	drbvrevngcrejkre
24	cqauqdumfbqdijqd
25	bpztpctleapchipc

Although this is tedious by hand, it is easy on a computer.

Kerckhoff's Principle

In 1883, Auguste Kerckhoffs asserted in *La Cryptographie Militaire* that cryptographers should assume that their adversaries know what encryption method is being used.

Therefore, security of the cryptosystem is determined by the security of the "key" (assuming that operators use the system correctly).

Improved Technology

The inventions of the telegraph, the radio, and the computer have made communication faster and increased the need for cryptography because adversaries can more easily intercept messages and decipher them.

Encryption machines were common in World War II, the most famous of which is the German Enigma. The capture of an Enigma machine was the subject of the popular historical fictional movie "U571" in 2000. It also mentioned in 2014 movie called "The Imitation Game".

Today, encryption is performed by computers and works on a binary alphabet.

Practice

Write a program to decrypt the following message which is encrypted using Caesar Cipher.

Zyvsmo: Grobo ny e vsfo? Wo: Gsdr wi zkboxdc. Zyvsmo: Grobo ny iyeb zkboxdc vsfo? Wo: gsdr wo. Zyvsmi: Grobo ny iye kvv vsfo? Wo: Dyqodrob. Zyvsmo: Grobo sc iyeb ryeco? Wo: Xohd dy wi xosrlybc ryeco. Zyvsmo: Grobo sc iyeb xosqrlybc ryeco? Wo: Iye gyx’d lovsofo wo sp S dovv iye. Zyvsmo: Xohd dy wi ryeco.

Next ...

Vigenere Cipher