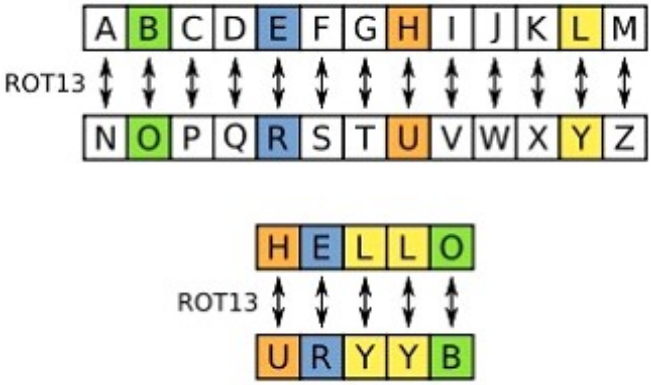
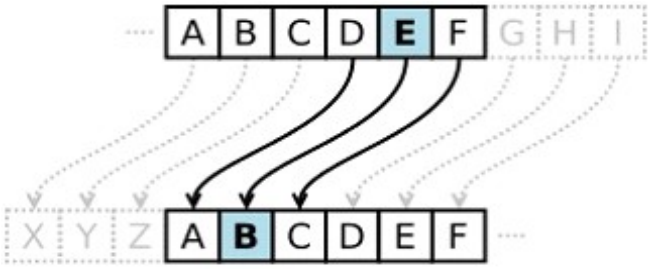
magazine printing the answer to a quiz upside down". ROT13 has inspired a variety of letter and word games on-line, and is frequently mentioned in newsgroup conversations. See diagram Below:



Rot 13 Cipher

The following are incorrect:
The Caesar cipher is a simple substitution cipher that involves shifting the alphabet three positions to the right. In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.



Caesar Cipher
Polyalphabetic cipher refers to using multiple alphabets at a time. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Vigen鑢e cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

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

Viginere Cipher
Transposition cipher is a different type of cipher. In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed. See the reference below for multiple examples of Transpositio Ciphers.

An exemple of Transposition cipher could be columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Both the width of the rows and the permutation of the columns are usually defined by a keyword. For example, the word ZEBRAS is of length 6 (so the rows are of length 6), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".

In a regular columnar transposition cipher, any spare spaces are filled with nulls; in an irregular columnar transposition cipher, the spaces are left blank. Finally, the message is read off in columns, in the order specified by the keyword. For example, suppose we use the keyword ZEBRAS and the message WE ARE DISCOVERED. FLEE AT ONCE. In a regular columnar transposition, we write this into the grid as Follows:

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E	Q	K	J	E	U

Transposition Cipher

Providing five nulls (QKJEU) at the end. The ciphertext is then read off as:

EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE

Reference(s) used for this question:

http://en.wikipedia.org/wiki/ROT13
http://en.wikipedia.org/wiki/Caesar_cipher
http://en.wikipedia.org/wiki/Polyalphabetic_cipher
http://en.wikipedia.org/wiki/Transposition_cipher

QUESTION 793
Which of the following standards concerns digital certificates?

A. X.400
B. X.25
C. X.509
D. X.75

Correct Answer: C
Explanation:
X.509 is used in digital certificates. X.400 is used in e-mail as a message handling protocol. X.25 is a standard for the network and data link levels of a communication network and X.75 is a standard defining ways of connecting two X.25 networks.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 164).

QUESTION 794
Which of the following is best provided by symmetric cryptography?

A. Confidentiality
B. Integrity
C. Availability
D. Non-repudiation

Correct Answer: A
Explanation:
When using symmetric cryptography, both parties will be using the same key for encryption and decryption. Symmetric cryptography is generally fast and can be hard to break, but it offers limited overall security in the fact that it can only provide confidentiality.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 2).

QUESTION 795
A code, as is pertains to cryptography:

A. Is a generic term for encryption.
B. Is specific to substitution ciphers.
C. Deals with linguistic units.
D. Is specific to transposition ciphers.

Correct Answer: C
Explanation:

Historically, a code refers to a cryptosystem that deals with linguistic units:
words, phrases, sentences, and so forth. Codes are only useful for specialized circumstances where the message to transmit has an already defined equivalent ciphertext word.
Source: DUPUIS, CI?ment, CISSP Open Study Guide on domain 5, cryptography, April 1999.

QUESTION 796
In what type of attack does an attacker try, from several encrypted messages, to figure out the key used in the encryption process?

A. Known-plaintext attack
B. Ciphertext-only attack
C. Chosen-Ciphertext attack
D. Plaintext-only attack

Correct Answer: B
Explanation:
In a ciphertext-only attack, the attacker has the ciphertext of several messages encrypted with the same encryption algorithm. Its goal is to discover the plaintext of the messages by figuring out the key used in the encryption process. In a known-plaintext attack, the attacker has the plaintext and the ciphertext of one or more messages. In a chosen-ciphertext attack, the attacker can chose the ciphertext to be decrypted and has access to the resulting plaintext.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 8: Cryptography (page 578).

QUESTION 797
Which of the following terms can be described as the process to conceal data into another file or media in a practice known as security through obscurity?

A. Steganography
B. ADS - Alternate Data Streams
C. Encryption
D. NTFS ADS

Correct Answer: A
Explanation:
It is the art and science of encoding hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message or could claim there is a message.

It is a form of security through obscurity.

The word steganography is of Greek origin and means "concealed writing." It combines the Greek words steganos (), meaning "covered or protected," and graphei () meaning "writing."

The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages will appear to be (or be part of) something else:
images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable, will arouse interest, and may in themselves be incriminating in countries

where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.
It is sometimes referred to as Hiding in Plain Sight. This image of trees blow contains in it another image of a cat using Steganography.
ADS Tree with Cat inside

This image below is hidden in the picture of the trees above:

Hidden Kitty
As explained here the image is hidden by removing all but the two least significant bits of each color component and subsequent normalization.

ABOUT MSF and LSF

One of the common method to perform steganography is by hiding bits within the Least Significant Bits of a media (LSB) or what is sometimes referred to as Slack Space. By modifying only the least significant bit, it is not possible to tell if there is an hidden message or not looking at the picture or the media. If you would change the Most Significant Bits (MSB) then it would be possible to view or detect the changes just by looking at the picture.

A person can perceive only up to 6 bits of depth, bit that are changed past the first sixth bit of the color code would be undetectable to a human eye.

If we make use of a high quality digital picture, we could hide six bits of data within each of the pixel of the image. You have a color code for each pixel composed of a Red, Green, and Blue value. The color code is 3 sets of 8 bits each for each of the color. You could change the last two