計算機概論　　課堂測驗六(Ch.15,16)　　2012/01/12

系級：_____學號：_____姓名：_____

一、選擇題 (每題 4 分，答案不一定只有一個; 如果全錯，則請寫"全錯")

( ) 1. _____ is an example of lossy compression.
(A) Huffman encoding (B) MP3
(C) MPEG (D) Lempel Ziv encoding

( ) 2. LZ encoding is an example of a category of algorithms called _____.
(A) dictionary-based encoding (B) lossy compression
(C) Huffman encoding (D) run-length encoding

( ) 3. In JPEG encoding, the blocking process breaks the original picture into small blocks of _____ pixel blocks.
(A) 2×2 (B) 4×4 (C) 8×8 (D) 16×16

( ) 4. 以下有關 Huffman encoding 的敘述，那些是**錯**的？
(A) 主要應用於 WINZIP、WINRAR 等壓縮程式
(B) 適用於亂數產生的、或已壓縮的資料
(C) Huffman code can compress a file with the minimum number of bits.
(D) 需要讀取資料二次才能編碼。

( ) 5. Symmetric key encryption 比起 Asymmetric key encryption 來，其優點為：
(A) the short amount of time required for encryption/decryption
(B) a smaller number of keys is needed
(C) integrity is preserved
(D) everyone knows all the keys

( ) 6. Denial of services is a type of attack that threats to _____.
(A) availability (B) confidentiality (C) integrity (D) nonrepudiation

( ) 7. DES is an example of a modern
(A) symmetric-key cipher (B) asymmetric-key cipher (C) digital signature
(D) digital watermarking

( ) 8. In the digital signature method, the sender uses the _____ key to encrypt the message.
(A) prime (B) secret (C) private (D) public

( )9. 數位簽章兩種方法中「Signing the digest」比起「Signing the whole document」來，主要的優點是
(A) 保密效果比較差 (B) 處理較快 (C) keys 的數量較多
(D)較不適合網際網路使用

( ) 10. MD5 and SHA-1 are two common _____ for signing a digest of a document.

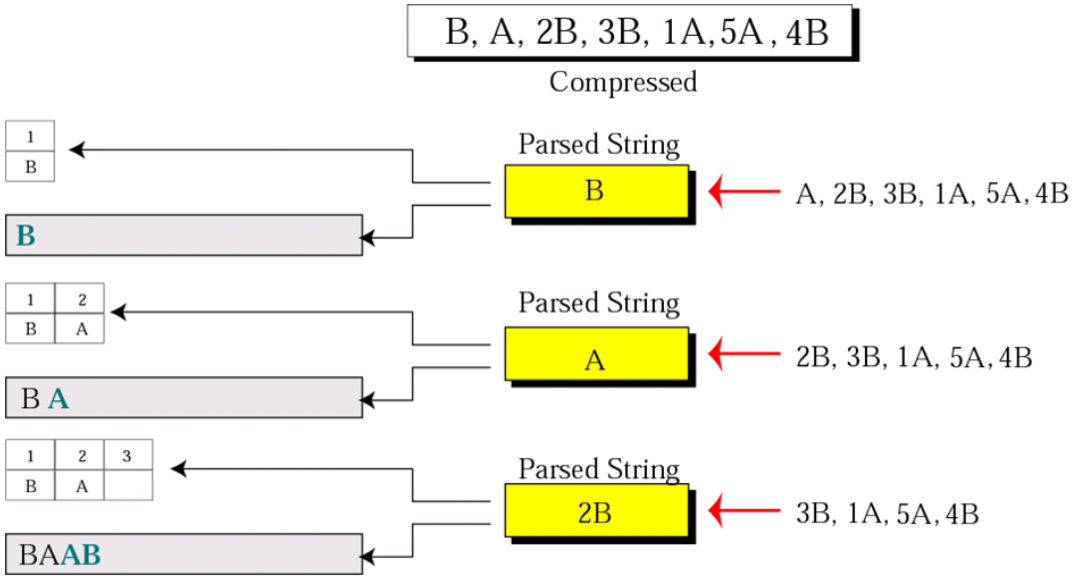
(A) subkey generators (B) certificate authorities (C) hash functions
(D) digital signatures

二、 填空題 (每格 5 分)

1. 假設一個文件中只含 4 個英文字母，其出現頻率如右表所示，請問其 Huffman code 的平均長度為何？(Suppose the four letters have the indicated frequency in a message. What is the average Huffman code length?)

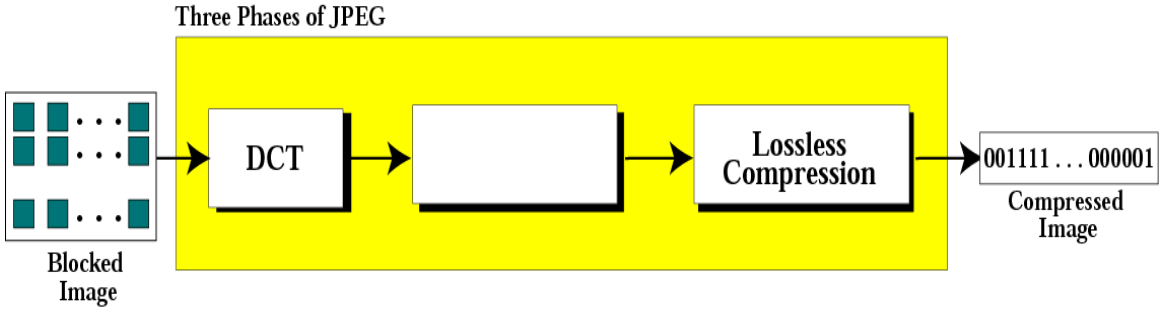
Key	Frequency
A	7
B	3
C	4
D	1
Total	**15**

2. 下圖是一個 Lempel Ziv decoding(解碼)的前 3 個步驟的示意圖，其中左邊"3"的下方有一空格，請填空。



3. 請問上題中最後 uncompressed 的 message 為何？

4. 下圖中間有一空格，請填空。



5. 請問上題圖中右邊的 Lossless Compression 用的是那一種壓縮法？

_____

6. 請將下列 2×2 矩陣的 inverse discrete cosine transform (IDCT)求出來。

8	6
5	-2

_____。

7. 請將下列 8×8 矩陣的 discrete cosine transform (DCT)求出來。

9	9	9	9	9	9	9	9
9	9	9	9	9	9	9	9
9	9	9	9	9	9	9	9
9	9	9	9	9	9	9	9
9	9	9	9	9	9	9	9
9	9	9	9	9	9	9	9
9	9	9	9	9	9	9	9
9	9	9	9	9	9	9	9

_____。

8. 下圖是 JPEG 推薦的量化矩陣(Quantization matrix)，請問它的作用為何？

_____

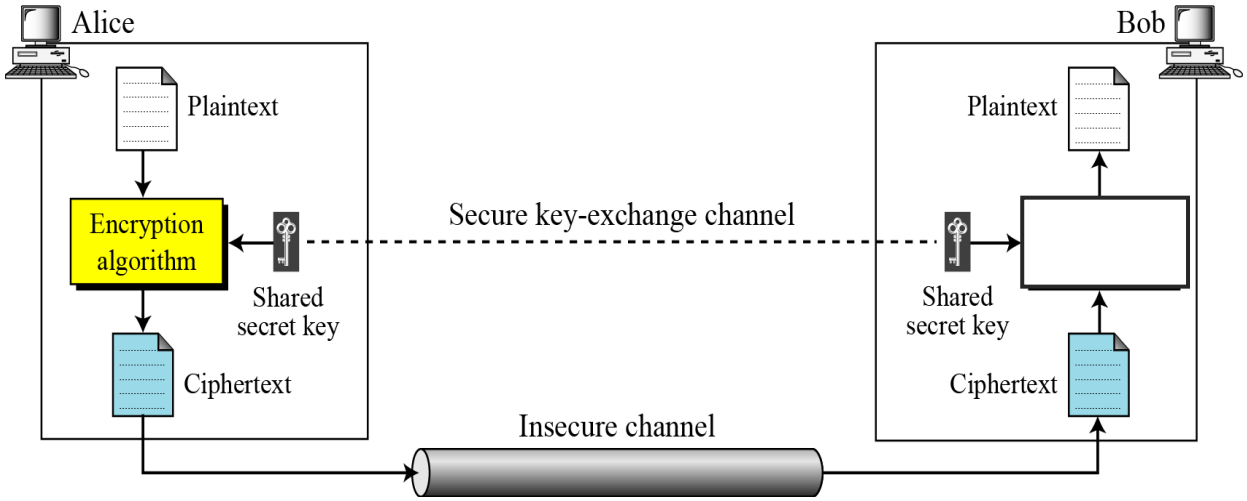
16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

9. MPEG frames有三種：I-frames、P-frames、_____。

10. Encrypt the message "attack" using the Caesar ciphers (凱撒加密法) .

_____

11. 下圖是 SYMMETRIC-KEY CRYPTOGRAPHY 的示意圖，其中右邊有一挖空部份，請填空。



12. SA 加密演算法之安全性取決於_____分解之困難度。

13. Consider the following RSA example: The public key is N=55 and e=3. Encrypting the plaintext F_1=6, we get the ciphertext C_1=_____. To break it, we find its private key d=_____. Suppose that a ciphertext C_2=2 is received, then the corresponding plaintext F_2=_____.(請算出值，若只列出公式則扣 2 分)

14. In the RSA algorithm, why can't Bob (the receiver) choose 1 as the public key *e*?

_____