**Answers and grading comments for Assignment 4 – Week 4**

**DO NOT COPY, SHARE OR REPRODUCE THIS MATERIAL AS IT CAN GET YOU EXPELLED FROM M.U.M.**

**(1) In a Caesar cipher, the encryption function is the same as the decryption function.**  
  
a) True  
b) False

**ANS: b**  
Most students got this one. The encryption function shifts right, the decryption function shifts left.

**(2) Let's say that the plaintext "hello" is enciphered as "zbabh". What kind of cipher is this? (It is one of the three choices given)**  
  
a) substitution  
b) transposition  
c) product (both substitution and transposition)

**ANS: c**

If it were pure substitution, the substitution for "l" would result in two letters being next to each other. If it were pure transposition, there would not be a "z", "b", or "a" in the result. Hence it must be a product cipher.

**(3) Rosetta stone is an example of which type of attack?**  
a) Ciphertext only (have only the ciphertext)  
b) Known plaintext (have the ciphertext for a known plaintext)  
c) Chosen plaintext (can generate ciphertext for any plaintext)

**ANS: b**

**(4) Which of the following are true about sending a PGP message from Alice to Bob?**

a) The plaintext is enciphered with Alice's public key  
b) The plaintext is enciphered with Alice's private key  
c) The plaintext is enciphered with Bob's public key  
d) The plaintext is enciphered with Bob's private key  
e) The plaintext is enciphered using a secret key  
f) The plaintext is compressed before it is enciphered  
g) The plaintext is compressed after it is enciphered  
h) The plaintext is signed using Bob's public key  
i) The plaintext is signed using Alice's public key  
j) The plaintext is signed using Alice's private key

**ANS: e, f, j**

a. The plaintext cannot be enciphered with Alice's public key because Bob does not have her private key  
b. The plaintext cannot be enciphered with Alice's private key, because any one with her public key could decipher it  
c. The plaintext \*\*could\*\* be enciphered with Bob's public key, but public keys are generally not used to encipher large amounts of data. Instead a symmetric key is generated and used to encipher the data. The symmetric key is then enciphered with Bob' public key  
d. The plaintext cannot be enciphered with Bob's private key because Alice does not have it.  
h,i. You never sign using a public key because that is available to everybody.  
  
   
**(5) Briefly describe why a symmetric cipher is never used for a digital signature.**

**ANS**:  Several reasons.  
1. The receiver would have to have a copy of the key used to encode the hash of the message (the key could not be made public because everybody could use it). This would be a key management nightmare.  
2. More importantly, the receiver could modify the message and resign it because he has the key used to encrypt the hash.  
You needed to explain what the problem was with sharing the same key between sender and receiver.

**(6) The key MUST be of the same length as that of the message in which cipher technique?**  
a) Rail-fence  
b) Vegenere  
c) One Time pad  
d) Casear cipher

**ANS: c**

**(7) What is the most important difference between symmetric and asymmetric cryptography?**

**ANS**: In symmetric cryptography there is only one key; in asymmetric cryptography there are two keys, one used to encrypt and the other used to decrypt.

**(8) If I get a message from someone that’s encrypted with my public key, then I’m assured about Origin Integrity.**  
a) True  
b) False

**ANS: b**

**(9) In what way does the Electronic Code Book mode of DES behave like a substitution cipher rather than a product cipher?**

**ANS:** Two identical 64 bits blocks will be encrypted identically.  
  
  
**(10) The cipher text for word “SECURITY” using a rail-fence cipher with a key of 3 is:**  
a) SUTERYCI  
b) SCRTEUIY  
c) YTIRUCES  
d) UGEWTKVA

**ANS: THE CORRECT ANSWER SHOULD BE "SREUIYCT"**

**(11) Vegenere is a :**  
a) Substitution cipher  
b) Transposition cipher

**ANS: a**

**(12) Keeping the enciphering and deciphering algorithm secret would violate which design principle?**

a) Principle of least privilege  
b) principle of fail-safe defaults  
c) principle of open design  
d) principle of complete mediaion  
e) principle of separation of privilege  
f) principle of psychological acceptibility  
g) principle of least common mechanism  
h) principle of economy of mechanism

**ANS: c**

**(13) Given enough time the private key can be derived from the public key.**  
a) True  
b) False

**ANS: a**

**DO NOT COPY, SHARE OR REPRODUCE THIS MATERIAL AS IT CAN GET YOU EXPELLED FROM M.U.M.**