**Computer Security – IV1013**

**Quiz 1**

1, Compute the multiplicative inverse of 5 in **Z**21.

17

2, Eve has an antenna that can pick up Alice’s encrypted cell phone conversations. What type of attack is Eve employing?

Ciphertext-only attack ?

3, What is 716 mod 11?

4

4,

6, 9, 7

5, Why can’t Bob use the pair (1,*n*) as an RSA public key, even if *n*=*pq*, for two large primes, *p* and *q*?

1 doesn’t encrypt

6,

7 254 329

7, Assume that the Hill cipher matrix *K* is

CAT = 2 0 19 Cipher = 24 17 19

8, What is 7120 mod 143?

1

9,

Sub for 12 = 7

Sub for 7 = 11

Sub for 2 = 15

10,

11,

12,

13,

128 = 3.40E38

192 = 6.28E57

256 = 1.16E77

14, What is the encryption of the string THELAZYFOX using the Caesar cipher (with three shift steps)?

WKHODCBIRA

15, Show the result of an Elgamal encryption of the message *M*=8 using *k*=4 for the public key (*p*,*g*,*y*)=(59,2,25):

(16, 6)

16,

An attacker has an encrypted message and knows the plain text is in ASCII-form. The attacker is aware of the encryption algorithm and that the key is 128 bit long. In a brute-force attack, what is the minimum number of characters of the plain-text in order to be able to find the secret key?

152

17,

Explain why non-forgeability and non-mutability imply non-deniability for digital signatures.

Non-mutability implies non-repuditation which makes  it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message.

18,

Explain the strengths and weaknesses of using symmetric encryption, like AES, versus a public-key cryptosystem, like RSA.