Computer Security – IV1013
Quiz 1

1, Compute the multiplicative inverse of 5 in $\mathbf{Z}_{21}$.

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 7^{16} 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

$$K = \begin{bmatrix} 19 & 15 & 2 \\ 17 & 21 & 21 \\ 8 & 11 & 7 \end{bmatrix}$$

CAT = 2 0 19 Cipher = 24 17 19

8, What is 7^{120} mod 143?

1

9,

Sub for 12 = 7

Sub for 7 = 11

Sub for 2 = 15

10,

11,

$$K = \begin{bmatrix} 19 & 15 & 2 \\ 17 & 21 & 21 \\ 8 & 11 & 7 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 8 & 11 & 13 \\ 17 & 13 & 23 \\ 5 & 19 & 16 \end{bmatrix}$$

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-repudiation which makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message. Non-mutability means that it's not possible to reuse a signature from a previous message.

Non-forgeability means it's not possible to counterfeit a signature. I.e. only the valid user can sign with the valid signature.

If both non-mutability and non-forgeability holds the signature cannot be denied.

Non-forgeability and non-mutability imply non-deniability because if it's impossible to counterfeit your signature and at the same time it's not possible to use a previously used signature then it must be the valid user. I.e. you cannot deny that you have signed.

18,
Explain the strengths and weaknesses of using symmetric encryption, like AES, versus a public-key cryptosystem, like RSA.

Symmetric cryptography primary purpose is to encrypt data and allow decryption by anyone that has the knowledge of the encrypting key.

Pros

- **Simple:** Easy to carry out. All users have to do is specify and share the secret key and then begin to encrypt and decrypt messages. Single-key encryption does not require a lot of computer resources when compared to public key encryption.

Cons

Sharing the secret key in the beginning is a problem in symmetric key encryption. It has to be exchanged in a way that ensures it remains secret. A new shared key has to be generated for communication with every different party. This creates a problem with managing and ensuring the security of all these keys.

Asymmetric cryptography primary purposes are to use a "public" key to encrypt data to the owner of a "private" key, and also to digitally sign (authenticate) messages

Pros

It solves the problem of distributing the key for encryption.Everyone publishes their public keys and private keys are kept secret. Public key encryption allows the use of digital signatures which enables the recipient of a message to verify that the message is truly from a particular sender.

Cons

Slow: Public key encryption is slow compared to symmetric encryption. Not feasible for use in decrypting bulk messages. It requires a lot more computer supplies compared to single-key encryption.