**Name:** Nguyễn Việt Hoàng **Student's ID:** B22DCVT214

# QUIZ FOR LECTURE 3

**P1. (30 pts) Determine each statement is "True" or "False"**

1. T F Public key encryption is a general-purpose technique that has rendered symmetric encryption obsolete.
2. T F During key exchange, the private keys do not have to be used at all.
3. T F Digital signature is not a type of application of public key
4. T F RSA is at least 100 times slower than DES
5. T F Factoring large numbers is easy especially when using RSA
6. T F When Bob wants Alice's public key, he must give his private key

**P2 (20 pts)**: Considering a public key crypto system, Bob chooses *p=5, q=7,*

2.1 (5 pts) is it OK if Bob selects $e = 9$?

**Your answer (Yes or No, and Why):**

No, because gcd(e,z) must equal to 1, while gcd(9,24) equal 3

2.2 (5 pts) is it OK if Bob select $e = 5$, the $d = 77$

**Your answer (Yes or No, and Why):**

Yes, since gcd(e,z) = gcd(5,24) = 1 so e = 5 is valid, and (e*d) mod z = 1, and (5*77) mod 24 = 1 so d = 77 is valid

2.3 (10 pts) Let now assume that Bob select $e = 5$, the $d = 29$, he wants to encrypt a plaintext message m = 3, what is the ciphertext? (***show your work***)

n = p * q = 5 * 7 = 35
c = m^e mod n
= 3^5 mod 35
= 33
The ciphertext is 33

**P3 (20 pts) Let now assume Bob chooses *p=1993, q=2293,***

a. (5 pts) What is $n$ = p * q = 1993 * 2293 = 4569949

b. (5 pts) Approximately, how many prime numbers between one and $n$ ? Approximately x/lnx = 2.98 * 10^5

b. (10 pts) If an attacker, who know the Bob's public key, want to brute force to find the private key, on average, how many prime number does that attacker has to try? Select the closet approximated number

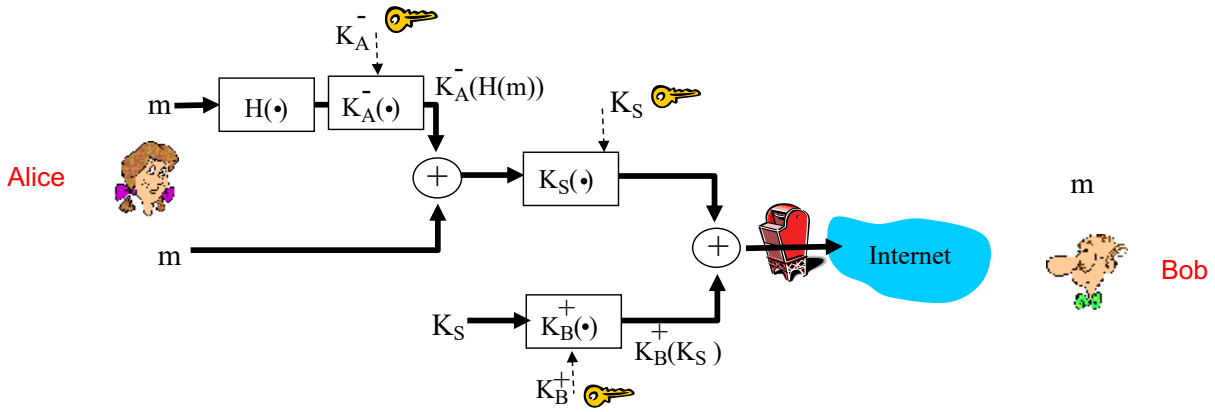
(1) 200

(2) 2,000

(3) 200,000

Attacker need to try from 1 to sqrt(4569949) = 2134
Number of primes number under 2138 is about 2134/ln(2134) = 279
On average, attacker would have to try half of those number, which is about 140
So the answer is option (1) 200

**P4 (30pts):** Alice wants to send a secure message, m, to Bob using the system as bellow.




A. (10 pts) Complete the diagram of the receiver side (in the next page) so that Bob can recover the original message, *m*.

B. (20 pts) Decide "True" or "False" for the following statements (5 pts for each correct answer)

1. ( T / F ) Alice encrypts the message by using a symmetric key
2. ( T / F ) The message confidentiality and sender authentication can be guaranteed by encryption and Hash function, message integrity, however, is not guaranteed.
3. ( T / F ) Bob and Alice need share the secret key in advance
4. ( T / F ) Alice can guarantee that only Bob is able to decrypt the message.