The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security
Week 10 Workshop – 10th and 12th May 2021

1. In 1985, T. Elgamal announced a public-key scheme based on discrete logarithms, closely related to the Diffie-Hellman key exchange technique introduced in 1976.
The global elements of ElGamal scheme are a q and α, where q is prime, and α is a primitive root of q. A user A selects a private key X_A and calculates a public key $Y_A = \alpha^{X_A} \bmod q$.

User A encrypts a plaintext M < q intended for user B as follows.
1. Choose a random integer k such that $1 \le k \le q-1$.
2. Compute $K = (Y_B)^k \bmod q$.
3. Encrypt M as the pair of integers (C_1, C_2) where $C_1 = \alpha^k \bmod q$ and $C_2 = K \cdot M \bmod q$.

User B receives the ciphertext (C_1, C_2) and recovers the plaintext as follows:
1. Compute $K = (C_1)^{X_B} \bmod q$. (i.e. use C_1 to recover K)
2. Compute $M = (C2 \cdot K^{-1}) \bmod q$. (i.e. use K and C_2 to recover M)

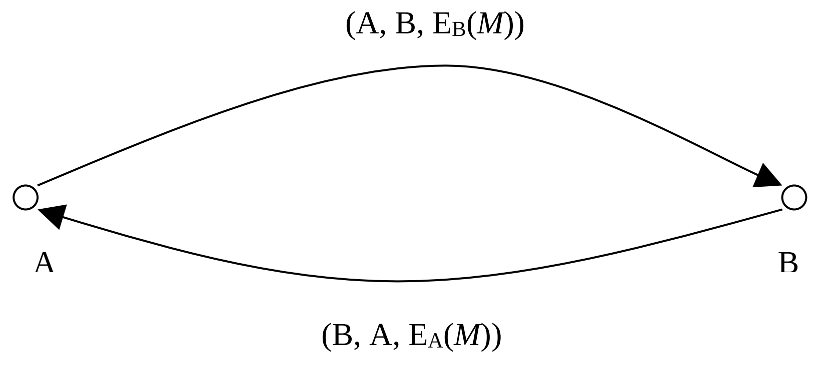
Show that the system works. (i.e. show that the decryption process recovers the plaintext)

2. In the RSA public-key encryption scheme, each user has a public key e and a private key d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe?

3. In an RSA system, the public key of one user is (31, 3599). What is the user's private key?

4. Prove that RSA public system works correctly even when $\gcd(M, n) \neq 1$.

5. Show how an active wiretapper could break the following scheme to determine M. Users Alice and Bob exchange a message M using the following public-system protocol:
   a. Alice encrypts M using Bob's public key and sends the encrypted message $E_B(M)$ together plaintext stating both Alice's and Bob's identity, i.e., $(A, B, E_B(M))$
   b. Bob deciphers the ciphertext and replies to Alice with $(B, A, E_A(M))$.



6. Suppose users Alice and Bob exchange a message M in a conventional system using a trusted third party S and the protocol given below. Show how an active wiretapper could break the scheme to determine M by replaying $E_A(R)$.

a. Alice generates a random number R and sends to S her identity A, destination B and $E_A(R)$.
b. S responds by sending $E_B(R)$ to Alice.
c. Alice sends $(E_R(M), E_B(R))$ to Bob.
d. Bob decrypts $E_B(R)$ and uses R to decrypt $E_R(M)$ and get M.