CPSC 418 / MATH 318 — Introduction to Cryptography
ASSIGNMENT 3

Name: Artem Golovin
Student ID: 30018900

Problem 1 — A modified man-in-the-middle attack on Diffie-Hellman, 12 marks

(a) Let $y_a \equiv (g^a)^q \pmod{p}$, $y_b = (g^b)^q \pmod{p}$ and key K:

i. *Alice* receives malicious y_a and sends it to *Bob*.

ii. *Bob* receives malicious y_b and sends it to *Alice*.

iii. *Alice* computes $K \equiv y_b^a \equiv ((g^b)^q)^a \pmod{p}$

iv. *Bob* computes $K \equiv y_a^b \equiv ((g^a)^q)^b \pmod{p}$

v. *Alice* and *Bob* get the same key K, because:

$$y_b^a \equiv ((g^b)^q)^a \equiv g^{bqa} \equiv g^{aqb} \equiv ((g^a)^q)^b \equiv y_b^a \pmod{p}$$

(b) ???

(c) In this version, *Mallory* does not have to pick a number e, where $1 < e < p$. Therefore, by knowing values $g^a \pmod{p}$ and $g^b \pmod{p}$, *Mallory* is more likely to compute $g^{abq} \pmod{p}$, which is a private key used by *Alice* and *Bob*.

Problem 2 — RSA and binary exponentiation, 24 marks

(a) ok

Problem 3 —

(a) ok

Problem 4 — The ElGamal public key cryptosystem is not semantically secure, 10 marks

Proof. By definition, a PKC is polynomially secure if no passive attacker can in expected polynomial time select two plaintexts M_1 and M_2 and then correctly distinguish between $E(M_1)$ and $E(M_2)$, where $E(M_1)$ and $E(M_2)$ are encryptions of M_1 and M_2 respectively with probability $p > \frac{1}{2}$.

However, it is given that $Mallory$ can assert whether $C = E(M_1)$ or $C = E(M_2)$ in polynomial time using modular exponentiation by Euler's Criterion with probability $p' = 1$, $p' > p$. It contradicts the definition of polynomially secure PKC, and therefore shows that ElGamal is not semantically secure. □

Problem 5 —

(a) ok