Introduction to Cryptography: Assignment 9

Group number 57

Elwin Tamminga s1013846

Lucas van der Laan s1047485

1

We work in the system of $x \mod 5791$

(a) $A = 137^{567} \equiv 1131$

(b) Shared key $K_{A,B} = B^a = 1262^{567} \equiv 682$

(c) We know that $g^b \equiv B$. So $137^b \equiv 1262$

$$\begin{aligned}
137^1 &\mod 5791 = 137 \\
137^2 &\mod 5791 = 1396 \\
137^3 &\mod 5791 = 149 \\
137^4 &\mod 5791 = 3040 \\
137^5 &\mod 5791 = 5319 \\
137^6 &\mod 5791 = 4828 \\
137^7 &\mod 5791 = 1262
\end{aligned}$$

So Bob's private key is $b = 7$.

(d) We are in a multiplicative cyclic prime group, which means that every value can only appear once, thus the private key is unique.

2

(a) The order of the cyclic group $G = 718$, because 719 is a prime number. The order of the cyclic sub-group $\langle g \rangle = 359$. So $359/718 = 0.5 = 50\%$ of the elements in G will be encoded as the same element in $\langle g \rangle$.

(b) The ciphertext is created with (C, A)
$A = g^a = 3^{17} \mod 719 = 573$
$C = M \times B^a = (96 \times 526^{17}) \mod 719 = 465$
So $(C, A) = (465, 573)$

(c) $M = C \times A^{q-b} = 113 \times 375^{359-13} \equiv 104 (\text{mod } 719)$.
This means that the message was "Bobby Subroto"

(d) Alice reused the same ephemeral key pair for the second message.
1st message: $104 \equiv 113 \times 375^{359-b} \mod 719$
2nd message: $M' \equiv 81 \times 375^{359-b} \mod 719$
$\frac{M'}{M} = \frac{C'}{C} \mod 719$
$\frac{M'}{104} = \frac{81}{113} \mod 719$

$$\begin{aligned} \frac{M'}{104} &\equiv \frac{81}{113} \\ 113M' &\equiv 81 \times 104 \\ 113M' &\equiv 8424 \\ 70 \times 113M' &\equiv 70 \times 8424 \\ M' &= 589680 \mod 719 = 100 \end{aligned}$$

To verify, we can decrypt the message using information that Bob would have.
$M' = C' \times A'^{q-b} = 81 \times 375^{359-13} \equiv 100 (\text{mod } 719)$.

3

(a) $M \in \langle g \rangle$. We can rewrite $M = g^m$ with $0 \leq m < q$, so $m \in \mathbb{Z}/q\mathbb{Z}$. This means $C = g^m \times g^{ab} = g^{m+ab}$. The private keys a and b are also in $\mathbb{Z}/q\mathbb{Z}$, so $c = m+ab \in \mathbb{Z}/q\mathbb{Z}$

(b) If $M = 1$, then $m = 0$ because $g^0 = 1$. Which means $c = ab$.
So if M_0 is encrypted, then $C = g^{m+ab}$ with $m = 0 \implies C = g^{ab} \implies c = ab$.
If M_1 is encrypted, then $g^c \neq g^{ab}$ but instead $g^c = g^{m+ab}$ with $m > 0$ so then $c \neq ab$.

(c) The probability $p = \frac{1}{2}$ because for one of the two messages we can not know if it is encrypted without solving the DDH problem. So only half of the time.

(d) A valid ElGamal encryption of M_b with public key B' is $C = B'^{a'} \times M_b$
In this case $B'^{a'} = g^{a'b'} = C'$
So $C = C' \times M_b$, which means that $(M_b \times C', A')$ is a valid ElGemal encryption.

(e) Pr$[\mathcal{B} = 1 | C' = g^{a'b'}] = \frac{1}{2}$+Adv$_{\mathcal{A}}$
Pr$[\mathcal{B} = 1 | C' \neq g^{a'b'}] = \frac{1}{2}$

(f) Adv$_B$ =Pr$[\mathcal{B} = 1 | C' = g^{a'b'}]$−Pr$[\mathcal{B} = 1 | C' \neq g^{a'b'}] = \frac{1}{2}$+Adv$_{\mathcal{A}} - \frac{1}{2}$ =Adv$_{\mathcal{A}}$