Assignment 11: Diffie-Hellman Key Exchange

Rajdeep Gill 7934493

ECE 3760 A01

March 21, 2025

1 Key Exchange Algorithm

We will pick a $q > 29$, so lets pick $q = 41$. We first check if q is prime, that is:

$$\begin{aligned} &2^{40} \bmod 41 = 1 \\ &\implies 2^{40} \equiv 1 \pmod{41} \\ &\implies q \text{ is prime} \end{aligned}$$

We let $p = 2q + 1 = 83$. We then check if p is prime:

$$\begin{aligned} &2^{82} \bmod 83 = 1 \\ &\implies 2^{82} \equiv 1 \pmod{83} \\ &\implies p \text{ is prime} \end{aligned}$$

Now, we pick a generator g that meets the following condition. We will start with $g = 3$:

$$\begin{aligned} g^{(p-1)/2} &\not\equiv 1 \pmod{p} \\ 3^{(83-1)/2} &\bmod 83 = 41 \\ &\implies 3^{41} \not\equiv 1 \pmod{83} \\ &\implies g = 3 \end{aligned}$$

So we can now share $g = 3$ and $p = 83$. Alice will now select a number **a** from $2, 3, 4, \ldots, 81$ and Bob will select a number **b** from $2, 3, 4, \ldots, 81$. Let Alice select $a = 5$ and Bob select $b = 7$ which they will keep secret. Then we calculate A and B to send to each other:

$$\begin{aligned} A = g^a \bmod p = 3^5 \bmod 83 = 77 \\ B = g^b \bmod p = 3^7 \bmod 83 = 29 \end{aligned}$$

Alice and Bob both receive A and B from each other. They then calculate the shared secret key:

$$\begin{aligned} \text{Alice: } B^a \bmod p = 29^5 \bmod 83 = 23 \\ \text{Bob: } A^b \bmod p = 77^7 \bmod 83 = 23 \\ \text{In Binary: } 0001\,0111 \end{aligned}$$

Now suppose we want to share a message $M = 11 = 1011\text{b}$ from Alice to Bob. Alice first XORs the message with the key and transmits the result:

$$\text{Encrypted Message: } 0000\,1011 \oplus 0001\,0111 = 0001\,1100$$

On the receiving end, Bob will XOR the received message with the shared key to decrypt the message:

$$\text{Decrypted Message: } 0001\,1100 \oplus 0001\,0111 = 0000\,1011$$

The Encrypted message is visible to anyone who intercepts it, but without the shared key, which is calculated using the private numbers a and b, the message is secure.