MATH 178 Homework #11

Tamir Enkhjargal

May 2019

My color: Red, My partner's color: Blue

Diffie-Hellman

1.

$g = 2,\ q = 677,\ a_A = 13.$

(a) My public key is $g^{a_A}(\text{mod}677) = 68$.

(b) Shared key $(g^{a_B})^{a_A}(\text{mod}q) = 286^{13}(\text{mod}677) = 197$

(c) $197/26 = 7,\ 197\%26 = 15,\ (a, b) = (7, 15)$.
$7 * 24 + 15 \text{ mod } 26 = 1 \rightarrow B$.
$7 * 14 + 15 \text{ mod } 26 = 9 \rightarrow J$. I send you '`BJ`'

2.

$p =$ `nextprime(10^24)` $= 100...007$
$g = 5$
$a_A = 200...069$
$g^{a_A} \text{ mod } p = 635...104$
Partner's public key: 258...269.
Our shared key: $258...269^{200...069} \text{ mod } 100...007 = 136...047$.
Reduced this down by $\text{mod}2^{16} = 38671$. This is our key.

3.

Ed's public key: 483...831.
Our shared key: $483...831^{200...069} \text{ mod } 100...007 = 867...073$.
Reduced this down by $\text{mod}2^{16} = 14233$. This is our key.
Decrypting the message using this key in CryptoSoft gets me '`Red state`'

4.

$q = x^{25} + x^3 + 1$
Public key: $x^{23}+x^{22}+x^{21}+x^{20}+x^{15}+x^{14}+x^{13}+x^{12}+x^{10}+x^9+x^7+x^6+x^4$
Private key: 8675309.
Running `Mod(public, q)^private` gets me:
$x^{23}+x^{22}+x^{20}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^9+x^8+x^6+x^5+x^3+x^2+x+1$.
Only using the coefficients from $a_{24}a_{23}...a_9$, we get our key as `0110100111111001`.
Decrypting the message with the key: '`Whit and Marty`'