Ungraded Homework Solutions

CSC 152 – Cryptography

Please notify me of any errors you find. If you need help, ask.

1) *Every element of a group generates a subgroup, and the size of the group is always a multiple of the size of the subgroup. For $\mathbb{Z}_7^*$ and $\mathbb{Z}_8^*$ determine the subgroups generated by each of its elements.*

In $\mathbb{Z}_7^*$: 1 generates $\{1\}$; 2 and 4 generate $\{1,2,4\}$; 3 and 5 generate $\{1,2,3,4,5,6\}$; and 6 generates $\{1,6\}$. In $\mathbb{Z}_8^*$ there are no even numbers: 1 generates $\{1\}$; 3 generates $\{1,3\}$; 5 generates $\{1,5\}$; 7 generates $\{1,7\}$. Note that because there is no value that generates all of $\mathbb{Z}_8^*$, it is not "cyclic" and therefore would not be useful in cryptography.

2) *Let's say Diffie-Hellman key-exchange is being done with generator $g = 4$ and prime $p = 467$. Note that g generates a subgroup of size 233. What is the key produced when the exponents chosen by the two parties are 400 and 134? What is the key produced when the exponents chosen by the two parties are 167 and 134? Why are the keys identical?*

The first key is $4^{400 \cdot 134} \bmod 467 = 161$. The second key is $4^{167 \cdot 134} \bmod 467 = 161$. Because 4 generates a subgroup of size 233, $4^{233} = 1$, so $4^{400 \cdot 134} = 4^{400 \cdot 134 \bmod 233} = 4^{10}$ and $4^{167 \cdot 134} = 4^{167 \cdot 134 \bmod 233} = 4^{10}$.

3) *A small elliptic curve group has elements from $\{(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid y^2 = x^3 + ax + b \bmod p\} \cup \{0\}$ where $a = 1$, $b = 6$ and $p = 11$. Let's say you choose 6 as your multiplier in a Diffie-Hellman key exchange and you receive $(5,9)$ as your communication partner's contribution. What is the shared key generated?*

We need to compute aB where $a = 6$ and $B = (5,9)$. This is easiest done with the double-and-add multiplication algorithm. Since $a = 6_{10} = 110_2$, this means the answer is $2(2(2\mathcal{O} + B) + B)$ or simply $2(2B + B)$. I wrote a small program to do point additions for me, from it I get $2B = (10,9)$, $2B + B = (7,2)$, and $2(2B + B) = (2,7)$.

4) *Let's say that you capture two ciphertexts encrypted using Elgamal in group $\mathbb{Z}_{31}^*$ using $g = 3$, and they are $(g^e \bmod p = 6, y = 17)$ and $(g^e \bmod p = 6, y = 25)$. Furthermore, you know that the first ciphertext is of plaintext $x = 21$. What is the second plaintext? This is essentially a math problem where I give you several pieces of information and you have to piece them together with the formulas and solve for the one unknown.*

The formula that relates y and x is $y = (g^d)^e x \bmod p$, so substituting the values we are given we have $17 = (g^d)^e 21$ and $25 = (g^d)^e x$ (all math mod 31). We can solve for $(g^d)^e$ in the first equation and substitute it into the second: $25 = 20x$. Solving for x we get $x = 9$.

5) *In Elgamal encryption a public key consists of the specification of a group, a generator, and a Diffie-Helman contribution. Let's say that my public key specifies group $\mathbb{Z}_{11}^*$, generator 2, and DH contribution 5. Tell me what grade you think you should get in this class A, B or C, and then encrypt it using my public key using A=2, B=3, C=4. If you need a random number during encryption, use 4.*

I'll do it for B. I choose my random DH exponent $e = 4$. This means the shared secret is $(g^d)^e = 5^4 \bmod 11 = 9$ and encryption of the value 3 is $(g^d)^e \cdot 3 \bmod 11 = 5$. I send my DH contribution $g^e \bmod 11 = 2^4 \bmod 11 = 5$ and enciphered value 5, so the ciphertext is the pair (5, 5).

6) *Find a generator of a subgroup of $\mathbb{Z}_p^*$. The bigger group should be a size that requires 15–17 bits to represent, and the subgroup should be a size that requires 5–7 bits to represent. The website `http://primes.utm.edu` may be of help. Along the way, you will establish the relationship $p = Nq + 1$. You can verify that your found generator g creates a subgroup of size q by querying WolframAlpha "order of g mod p"; it should reply q. Follow the process seen in class.*

A 5 bit prime number is 17, and 1000×17 is 16 bits, so I ask WolframAlpha "is (1000*17+1) prime". It's not, so I try "is (1002*17+1) prime". It's not. Eventually I find $(1008 \times 17 + 1) = 17137$ is prime. So, I'm

going to find a subgroup of size 17 in $\mathbb{Z}^*_{17137}$. The next step is to find an x where $g = x^{1008} \bmod 17137$ is not 1. In this case $g^{17} \bmod 17137$ will be 1 and g will generate the right size subgroup. I find it on the first try: $2^{1008} \bmod 17137 = 15617$. So, 15617 generates a size 17 subgroup. I can verify the subgroup using python `[15617**i % 17137 for i in range(1,18)]` generates the list `[15617, 14042, 8862, 16579, 8447, 13310, 7597, 2898, 16386, 10478, 10850, 10931, 7770, 14130, 12198, 1274, 1]` and "order of 15617 mod 17137" returns 17 on WolframAlpha.