M 375 – Homework 5

10.5.1

Given a prime number $p = 11$, a primitive root $a = 2$, and the public key of user A $e_A = 9$ the private key d_A for the key exchange algorithm is the solution of the equation:

$$a^{d_A} \equiv e_A \bmod p \text{, i.e. } 2^{d_A} \equiv 9 \bmod 11.$$

To solve this equation compute a lookup table for powers of 2 (mod 11):

d	$2^d \bmod 11$
1	2
2	4
3	8
4	5
5	10
6	9
7	7
8	3
9	6
10	1

$\rightarrow$

From row 6 we get $d_A = 6$.

10.5.2

Given private key of A $d_A = 6$, public key of A $e_A = 9$, and private key of B $d_B = 8$, public key $e_B = 3$.

$$K_{AB} = K_{BA} = e_B^{d_A} = e_A^{d_B} = 3^6 \equiv 9^8 \equiv 3 \bmod 11.$$

11.5.1

The prime *p* and the primitive root *a* are public, (C_1, C_2) is sent. Since $C_1 = a^k \Rightarrow k = \log_a C_1$. If we could compute the discrete logarithm in a quick way, we could get *k*. Furthermore $C_2 = K \cdot M \Rightarrow M = C_1 \cdot K^{-1}$ and $K = e^k$ (*e* is a public key), so we could get the message *M*.

11.5.2

The message $M = 30$. Prime number $p = 71$, primitive root $a = 7$. Public key $e = 3$. First part of the cryptogram $C_1 = 59$.

$$a^k = 7^k = 59 \bmod 71$$

Lookup table for *k*:

k	$7^k \bmod 71$
1	7
2	49
3	59
…	…

$\rightarrow$

So, $k = 3$.

$$K = e^k = 3^3 = 27$$

And

$$C_2 = K \cdot M = 27 \cdot 30 = 29 \bmod 71.$$

So, $C_2 = 29$.

Page 197, problem 10

On average $k = \frac{p}{2}$. That means $\log k = \log\left(\frac{p}{2}\right) = \log p - \log 2 = \log p - 1$. This kind of multiplication happens twice (for $C_1 = a^k$ and $K = e^k$) so the total amount of multiplications is $2 \cdot (\log p - 1) = 2\log p - 2 \approx 2\log p$.