Assignment 2 # 2.5, 2.7, 2.8

Simon Owens

2.5

$\mathbb{F}_p^* = \{1, \dots p-1\}$, $a \in \mathbb{F}_p^*$, $g^x \equiv a \bmod p$

$a^N \equiv 1 \pmod p$

Need to prove a has square root $\overset{\text{iff}}{\longleftrightarrow}$ $\log_g a \pmod{p-1}$ is even

Suppose $x = \log_g a$. If $x = 2k$ is even, then $g^x = g^{2k}$
$= (g^k)^2$
is square.

Suppose say x is odd. If that were the case then $x = 2k+1$, and say g^x is a square mod p, ex $g^x \equiv c^2 \bmod p$. Lets now use little Fermat's theorem.

$$c^{p-1} \equiv 1 \bmod p \bmod p$$
$$\equiv (c^2)^{\frac{p-1}{2}} \bmod p$$
$$\equiv (g^x)^{\frac{p-1}{2}} \bmod p$$
$$\equiv (g^{2k+1})^{\frac{p-1}{2}} \bmod p$$
$$\equiv g^{k(p-1)} \cdot g^{\frac{p-1}{2}} \bmod p$$

Use definition from theorem that says

$$g^{k(p-1)} \equiv (g^{p-1})^k \equiv 1^k \equiv \underline{1 \bmod p}$$

Substitute in

$1 \bmod p \cdot g^{\frac{p-1}{2}} \bmod p$

$g^{\frac{p-1}{2}} \equiv 1 \bmod p$ which is a contradiction that g is supposed to be a primitive root. This means every odd power of g is not a square modulo p.

2.7

$A \equiv g^a \bmod p$ and $B \equiv g^b \bmod p$

Input a, b, C

output 0 if $a \cdot b \neq C$

$a \cdot b = C$

C? $C \stackrel{?}{\equiv} g^{ab} (\bmod p)$ ⟸ the question

a) If you know g, g^a, and g^b then this gets you g^{ab}. You can compare the value of g^{ab} with C and check if they are equivalent

b) We only know how to solve DH computational problem to get the DH decision problem. Nobody knows how to just solve DH decision problem.

2.8

$p = 1373$ base $(g) = 2$

a) Alices picks $a = 947$

so $A \equiv 2^{947} \bmod 1373 \equiv 177 \bmod 1373$

Alice public key is $\boxed{177}$

b) Bob chooses $b = 716$ ... $B \equiv 469 \bmod 1373$

Alice encrypts message $m = 583$ using $k = 877$

$C_1 \equiv 2^{877} \equiv 719 \bmod 1373$

$C_2 \equiv 583 \cdot 469^{877} \equiv 623 \bmod 1373$ therefore

$(C_1, C_2) = (719, 623)$

c) $(C_1, C_2) = (661, 1325)$

$(C_1^a)^{-1} \cdot C_2 \equiv (661^{299})^{-1} \cdot 1325 \equiv 645^{-1} \cdot 1325 \equiv 794 \cdot 1325 \equiv 332 \bmod 13$

which makes $\boxed{m = 332}$ the key is $K = 566$

D) $2^b \equiv 893 (\bmod 1373)$ $\boxed{b = 219}$ now we have bobs private key

$(C_1^a)^{-1} \cdot C_2 \equiv (693^{219})^{-1} \cdot 793 \equiv 431^{-1} \cdot 793 \equiv 532 \cdot 793 \equiv 365 \bmod 137$

$K = 932$ which means $\boxed{m = 365}$