Kunal Mukherjee

2.5, 2.7, 2.8

2.5 $p > 2$, $g =$ primitive root $(\bmod p)$

a has a $\sqrt{a} \pmod p$ iff $x = \log_g(a) \pmod{p-1}$ & $2 \mid x$

$g^x = a$. If $x = 2k$ is even, then

$g^x = g^{2k} = (g^k)^2$ is a square.

But, if not, x is odd

$x = 2k+1$.

So, if g^x is square root mod p,

$g^x \equiv c^2 \pmod p$. Theorem 1.25, Fermat's little Theorem

$c^{p-1} \equiv 1 \pmod p$

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

But, $g^{k(p-1)} \equiv (g^{p-1})^k \equiv 1^k \equiv 1 \pmod p$

So, $g^{\frac{p-1}{2}} \equiv 1 \pmod p$

This contradicts the fact the g is a primitive root.
So, it shows that every odd power of g is not square root mod p.

2.7 a) This is a trivial answer. From g, g^a and g^b, we can compute g^{ab}. Then, we can simply compare the value of g^{ab} with C. And, just check if they are equal.

(b) I think it should be easy, because elliptic curve in 6.40 shows a simplier method of solving it but, currently, there is no sol, how to solve DH decision problem, without solving DHP.

2.8 A) $p = 1373$, $g = 2$

a) $a = 947$

$$A \equiv 2^{947} \pmod{1373}$$
$$\equiv 177 \pmod{1373}$$

so, $A = 177$

(b) $b = 716$, so $B = 2^{716} \equiv 469 \pmod{1373}$

$$c_1 = 2^{877} \equiv 719 \pmod{1373}$$
$$c_2 \equiv 583 \cdot 469^{877} \pmod{1373}$$
$$\equiv 623 \pmod{1373}$$

Alice sends $(c_1, c_2) = (719, 623)$

(c) $(c_1^a)^{-1} \cdot c_2 \equiv (661^{299})^{-1} \cdot 1325 \pmod{1373}$
$\equiv 645^{-1} \cdot 1325 \pmod{1373}$
$\equiv 794 \cdot 1325 \pmod{1373}$
$\equiv 332 \pmod{1373}$

$m = 332.$

(d) $2^b \equiv 893 \pmod{1373}$
so, $b = 219$, which is Bob's private key.

$(c_1^a)^{-1} \cdot c_2 \equiv (693^{219})^{-1} \cdot 793 \pmod{1373}$
$\equiv 431^{-1} \cdot 793 \pmod{1373}$
$\equiv 532 \cdot 793 \pmod{1373}$
$\equiv 365 \pmod{1373}$

$m = 365$