1. Determine the last two digits of 7^1002 using Euler's theorem. (2.5 points)

> $\phi(100) = \phi(25)\phi(4) = (25-5)*2 = 40$, so $7^{\phi(100)} = 7^{40} = 1 \text{ in } Z_{100}$
>
> $7^{1002} \equiv 7^{40*25} * 7^2 \equiv 7^2 \text{ in } Z_{100}$
>
> Hence, the last two digits are 49.

2. Determine [17^5,432,100 mod 11] (by hand) using Fermat's little theorem. (3.5 points)

> $17^{10} \equiv 6^{10} \equiv 1 \bmod 11$
>
> $17^{5,432,100} \equiv 17^{10*543,210} = 1 \bmod 11 :$

3. Perform El-Gamal encryption for the following setting and compute what Bob will output.

p: 9209

g: 3698

m: 204

Alice's random number a: 96

Bob's random number b: 106

H(x, y): 8-LSB of x XOR y

Es(k, m): k XOR m

LSB: Least Significant Bit(s)

(Hint: using slide # 24, you need to compute the following values.) (4 points)

sk = a

u = ga mod p

v = gb mod p

w = ub mod p

k=H(v,w)

c= Es(k,m)

output (v, c) = ?

> $sk = \alpha = 96$
>
> $u = g^{\alpha} = 3698^{96} \bmod 9209 = 5874$
>
> $v = g^{\beta} = 3698^{106} \bmod 9209 = 6825$
>
> $w = u^{\beta} = 5874^{106} \bmod 9209 = 4811$
>
> $k = H(v, w) = 01100010$

> $c = E_s(k, m) = 01100010 \text{ XOR } 11001100 = 10101110 = 174$