mj20873

Week 2 exercises

1) a) $5+8 = 3 \mod 10$

b) $8-13 = 12 \mod 23$

c) $13 \cdot 16 = 8 \mod 29$

d) $6^{-1} = 2 \mod 11$

e) 6^{-1} doesn't have an inverse mod 9

f) $\{1,2,3,4\}$ have an inverse mod 5

g) $\{1,5\}$ have an inverse mod 6

2) $p=37$, $g^{f}=2$, $g^{h}=5$, $d=6$

a) $ss = (g^{d} \mod p) = 5^{6} \mod_{37} = 11 \mod 37$

~~b) $pk_H = g^{d} \mod p$~~

b)

$pk_H = (g^{h}) \mod p$

$pk_H = g^{h+36n} \mod 37$

$= g^{h} \cdot \boxed{g^{36n} \mod 37}$

$= g^{h} \mod 37$

$g^{36n} \mod 37 = 1$ by Fermat's little theorem

lovely

1

c) $2^{h} = 5 \mod 37$, $h \to$ number mod 36

$36 = 3^2 \cdot 2^2 = 9 \cdot 4 \Rightarrow a = 9$, $b = 4$

$h \equiv f \mod 9$

$h \equiv e \mod 4$

so using Chinese remainder theorem and Fermat's theorem we get

$h = maf + nbe \mod 36$

where

$ma + nb = \gcd(a,b)$

~~$9m + 4b$~~

$9m + 4n = 1$

$\Rightarrow m = 1$

$n = -2$

$\Rightarrow h = 9f - 8e \mod 36$

$2^{9f - 8e \mod 36} \mod 37 = 5 \mod 37$

$2^{4 \cdot (-8e) \mod 36} \mod 37 = 9^{4} \mod 37$

2

$$2^{4 \bmod 36} \bmod 37 = 33 \bmod 37$$

$$2^{4 \bmod 36} \bmod 37 = 2^{9 \cdot 4 \bmod 36} \bmod 37$$

=> we only need to check

$e \in \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

=> $e = 5$

we do the same thing for

$$2^{9 \cdot 9 f \bmod 36} \bmod 37 = 5^{9} \bmod 37$$

<=>

$$2^{9 \bmod 36} \bmod 37 = 6 \bmod 37$$

-> repeats after 4

$f \in \{0, 1, 2, 3\}$

=> $f = 3$

(3)

$\Rightarrow h = 3 \cdot 9 - 8 \cdot 5 \bmod 37$

$\cancel{h = 24}$

$h = 23$

3) a) $p = 37$ $g = 2$

$sk = d = 7$

$pk = 2^7 \bmod 37 = 17$

$(p, g, pk) \to H$

$H \to (pk_H, enc_m) = (9, 13)$

$m = ?$

$m = enc_m / ss \bmod 37$

$= enc_m \cdot ss^{-1} \bmod 37$

m is also equal to $enc_m \cdot pk_H^{p-1-d}$ (easier to compute)

$ss = g^7 \bmod 37 = 16 \bmod 37$

$ss^{-1} = 16^{-1} \bmod 37 = 7 \bmod 37$

(4)

$\Rightarrow m = 13 \cdot 7 \mod 37$

$= 17 \mod 37$

b) $H \xrightarrow{(pk_H,\, enc_m) = (9, 8)} A$

$enc_m = m \cdot s_{HA} = 8 \mod 37$

$17 \cdot s_{HA} = 8 \mod 37$

$s_{HA} = \frac{8}{17} \mod 37$

$= 8 \cdot 17^{-1} \mod 37$

$= 8 \cdot 24 \mod 37$

$= 7 \mod 37$

good!

5

4) a) p prime $\Rightarrow \varphi(p) = p-1$

$\varphi(p)$ is the number of integers x between 1 and p s.t $(p, x) = 1$ → $\gcd(p, x) = 1$?

Sorry, I can't read your hand-writing

p is prime $\Rightarrow \varphi(p)$ is all numbers between 1 and p, including 1

$\Rightarrow \varphi(p)$ is $p-1$ qed

b) $\varphi(p) = p-1$

$\varphi(q) = q-1$

Between 1 and pq there are q numbers that are multiples of p $(p, 2p, \dots, qp)$ and p numbers that are multiples of q

$\Rightarrow \left.\begin{matrix}(p-1) \text{ numbers} \\ (q-1) \text{ numbers}\end{matrix}\right\}$ if we exclude pq

$\Rightarrow \varphi(pq) = pq - 1 - (p-1) - (q-1)$

$\varphi(pq) = pq - p - q - 1$

$= (p-1)(q-1)$ qed

6

7) p prime $\Rightarrow \varphi(p^2) = p(p-1)$

$$\underbrace{\{p, 2p \cdots \cancel{p^2} (p-1)p\}}$$

$(p-1)$ numbers that are multiples of p and are smaller than p^2

$$\Rightarrow \varphi(p^2) = p^2 - (p-1) - 1$$

$$= p^2 - p = p(p-1)$$

q.e.d.

5) a) $29a + 101b = 1$

using a python script that does the calculation I get $a = 7$, $b = -2$

b) $x = 5 \cdot 29 \cdot 7^a - 2 \cdot 101 \cdot 12^a \mod (29 \cdot 101)$

$= \cancel{55303}$

1520

$x \equiv 5 \mod 29$

$x \equiv 12 \mod 29$

using the Chinese Remainder theorem

6) a) $p = 307$

$q = 311$

$n = 307 \cdot 311$

$\varphi(n) = 306 \cdot 310$

$pk = (247, n)$

$sk = (d, n)$

$sk = (d, \varphi(n))$

$d = 247^{-1} \mod \varphi(n)$

$= 55303$

$sk = (55303, 94860)$

b) for each m_i we calculate

$dm_i = m_i^d \mod_n$ and we then concatenate the answers and split it in strings of ~~a~~ lenght 2. After maping those to the letters we get

THEANSWERISFORTYTWO!

c) Invalid public key

(X , 8)

↳ not a product of two primes

true

(0,0) → mathemathically impossible to use as a key

yes