Math 116 HW4 Jun Ryu

1) $\mathbb{F}_p^*$ has a primitive root

$\Rightarrow$ let g be this primitive root

then, g has order $p-1$ by definition

So, if we let $h = g^{\frac{p-1}{N}}$ (since $N \mid p-1$),

h has order N ✓

2) a) $7^x = 166$ in $\mathbb{F}_{433}$

order$(7) = 432 = 2^4 \cdot 3^3$

$p_1 = 2$, $e_1 = 4$, $p_2 = 3$, $e_2 = 3$

$g_1 = g^{p_1^{-e_1} N} = 7^{2^{-4} \cdot 432} = 7^{27}$

$\equiv 265 \pmod{433}$

$h_1 = h^{p_1^{-e_1} N} = 166^{27} \equiv 250 \pmod{433}$

$(g_1)^y = h_1 \Rightarrow (265)^y \equiv 250 \pmod{433}$

$y = 15$

So, $\log_{g_1}(h_1) = 15 \in \mathbb{Z}/16$

$g_2 = g^{p_2^{-e_2}N} = 7^{3^{-3}\cdot 432} = 7^{16}$
$\equiv 374 \pmod{433}$

$h_2 = 166^{16} \equiv 335 \pmod{433}$

$(374)^y \equiv 335 \pmod{433}$
$y = 20$

So, $\log_{g_2}(h_2) = 20 \in \mathbb{Z}/27$

So, we solve
$x \equiv 15 \pmod{16}, \quad x \equiv 20 \pmod{27}$

and it is easy to see that $\boxed{x = 47}$

b) $10^x = 243278$ in $\mathbb{F}_{746497}$

order(10) $= 746496 = 2^{10} \cdot 3^6$

$p_1 = 2, e_1 = 10, p_2 = 3, e_2 = 6$

$g_1 = 10^{2^{-10}\cdot 746496} = 10^{729} \equiv 4168$
$\pmod{746497}$

$h_1 = 243278^{729} \equiv 38277 \pmod{746497}$

$(4168)^y \equiv 38277 \pmod{746497}$
$y = 523$

So, $\log_{g_1}(h_1) = 523 \in \mathbb{Z}/1024$

$$g_2 = 10^{3^{-6} \cdot 746496} = 10^{1024} \equiv 674719 \pmod{746497}$$

$$h_2 = 243278^{1024} \equiv 389966 \pmod{746497}$$

$$(674719)^y \equiv 389966 \pmod{746497}$$

$$y = 681$$

So, $\log_{g_2}(h_2) = 681 \in \mathbb{Z}/729$

So, we have

$x \equiv 523 \pmod{1024}$, $x \equiv 681 \pmod{729}$,

giving us $\boxed{x = 223755}$

c) $2^x = 39183497$ in $\mathbb{F}_{41022299}$

Order$(2) = p-1 = 2^1 \cdot 29^5$

$p_1 = 2, e_1 = 1, p_2 = 29, e_2 = 5$

$$g_1 = 2^{2^{-1} \cdot 41022298} = 2^{20511149} \equiv 41022298 \pmod{41022299}$$

$$h_1 = 39183497^{20511149} \equiv 1 \pmod{41022299}$$

$(41022298)^y \equiv 1 \pmod{41022299}$

$y = 0$

So, $\log_{g_1}(h_1) = 0 \in \mathbb{Z}/2$

$g_2 = 2^{29^{-5} \cdot 41022298} = 2^2 \equiv 4 \pmod{41022299}$

$h_2 = 39183497^2 \equiv 11844727 \pmod{41022299}$

$4^y \equiv 11844727 \pmod{41022299}$

$y = 13192165$

So, $\log_{g_2}(h_2) = 13192165 \in \mathbb{Z}/_{20511149}$

So, we have

$x \equiv 0 \pmod{2}$, $x \equiv 13192165 \pmod{29^5}$

$\boxed{x = 33703314}$

3) a) Let $\gcd(e, p-1) = d$.

Let g be a primitive root in $\mathbb{F}_p$.

Thus, there exists $0 < k \leq p-1$ s.t.

$g^k \equiv x \pmod{p} \Rightarrow g^{ke} \equiv c \pmod{p}$

let $c = 1$ and we see that $(p-1) \mid ke$.

$\Rightarrow \frac{(p-1)}{d} \mid \frac{ke}{d}$

$\gcd\left(\frac{p-1}{d}, \frac{e}{d}\right) = 1 \Rightarrow \frac{(p-1)}{d} \mid k$

Thus, $k \in \left\{ \frac{p-1}{d}, 2\left(\frac{p-1}{d}\right) \ldots d\left(\frac{p-1}{d}\right) \right\}$

since we said $0 < k \leq p-1$.

$\Rightarrow$ there are d solutions ✓

b) Solutions will exist if

$de \equiv 1 \pmod{p-1}$ yields

values for d s.t. $x \equiv c^d \pmod p$.

Thus, if $e \mid p-1$, there will be

no corresponding value for d, and thus c.

So, we subtract those cases

to find the number of values for c. ✓

4) a) ciphertext $c = m^e \pmod N$

$$= 892383^{103} \pmod{2038667}$$

$$\equiv \boxed{415293} \pmod{2038667}$$

b) $N = 2038667 = 1301 \cdot 1567$

So, $\phi(N) = (1301-1)(1567-1)$

$$= 2035800$$

So, if we solve

$$ed \equiv 1 \Rightarrow 103d \equiv 1 \pmod{2035800}$$

we get $d \equiv \boxed{810367} \pmod{2035800}$

c) $M = c^d \pmod N$

$$\equiv 317730^{810367} \pmod{2038667}$$

$$\equiv \boxed{514407} \pmod{2038667}$$

5) a) $n-1 = 294408 = 2^3 \cdot 36801$

$k = 3,\ q = 36801$

Take $a = 2$,

$$2^{36801} \equiv 512 \pmod{294409}$$
$$\not\equiv 1 \text{ or } -1$$

$$2^{2\cdot 36801} \equiv 262144 \pmod{294409} \not\equiv -1$$
$$2^{4\cdot 36801} \equiv 1 \pmod{294409} \not\equiv -1$$

So, 2 is a Miller-Rabin witness
$\Rightarrow$ 294409 is composite ✓

b) $n-1 = 294438 = 2^1 \cdot 147219$
$k=1,\ q=147219$

Take $a=2$,
$$2^{147219} \equiv 1 \pmod{294439}$$
So, 2 is not a Miller-Rabin witness.

We use the same process:
take $a=3$:
$$3^{147219} \equiv -1 \pmod{294439} \quad \times$$
$a=5$:
$$5^{147219} \equiv 1 \pmod{294439} \quad \times$$

$a=7$: $7^{147219} \equiv 1 \pmod{294439}$ ✗

$a=11$: $11^{147219} \equiv 1 \pmod{294439}$ ✗

$a=13$: $13^{147219} \equiv -1 \pmod{294439}$ ✗

$a=17$: $17^{147219} \equiv 1 \pmod{294439}$ ✗

$a=19$: $19^{147219} \equiv 1 \pmod{294439}$ ✗

$a=23$: $23^{147219} \equiv -1 \pmod{294439}$ ✗

$a=29$: $29^{147219} \equiv -1 \pmod{294439}$ ✗

So, we found 10 numbers that are not Miller - Rabin witnesses $\Rightarrow$ 294439 is probably prime ✓

c) $n-1 = 118901508 = 2^2 \cdot 29725377$

$k=2,\ q = 29725377$

Take $a=2$:

$$2^{29725377} \equiv 7906806 \pmod{118901509}$$

$$2^{2\cdot 29725377} \equiv -1 \pmod{118901509} \quad \times$$

$a=3$:

$$3^{29725377} \equiv -1 \pmod{118901509} \quad \times$$

$a=5$:

$$5^{29725377} \equiv -1 \pmod{118901509} \quad \times$$

$a=7$:

$$7^{29725377} \equiv 7906806 \pmod{118901509}$$

$$7^{2\cdot 29725377} \equiv -1 \pmod{118901509} \quad \times$$

$a=11$:

$$11^{29725377} \equiv -1 \pmod{118901509} \quad \times$$

$a=13$:

$$13^{29725377} \equiv 1 \pmod{118901509} \quad \times$$

$a=17$:

$$17^{29725377} \equiv 7906806 \pmod{118901509}$$

$$17^{2\cdot 29725377} \equiv -1 \pmod{118901509} \quad \times$$

$a = 19$:

$$19^{29725377} \equiv 110994703 \pmod{118901509}$$

$$19^{2\cdot 29725377} \equiv -1 \pmod{118901509} \quad \times$$

$a = 23$:

$$23^{29725377} \equiv 110994703 \pmod{118901509}$$

$$23^{2\cdot 29725377} \equiv -1 \pmod{118901509} \quad \times$$

$a = 29$:

$$29^{2\cdot 29725377} \equiv 1 \pmod{118901509} \quad \times$$

So, we found 10 numbers that are not Miller-Rabin witnesses $\Rightarrow$ 118901509 is probably prime ✓

d) $n-1 = 118901520 = 2^4 \cdot 7431345$

$k = 4,\ q = 7431345$

Take $a = 2$:

$$2^{7431345} \equiv 45274074 \pmod{118901521} \not\equiv 1 \text{ or } -1$$

$2^{2 \cdot 7431345} \equiv 1758249 \pmod{118901521} \not\equiv -1$

$2^{4 \cdot 7431345} \equiv 1 \pmod{118901521} \not\equiv -1$

$2^{8 \cdot 7431345} \equiv 1 \pmod{11890152 1} \not\equiv -1$

So, 2 is a Miller-Rabin witness

$\Rightarrow$ 11890 1521 is composite ✓

6) a) Do the Miller-Rabin algorithm to check for the compositeness of a number $\rightarrow$ there are nontrivial solutions.

Then, for any $a \in (\mathbb{Z}/p\mathbb{Z})^*$, check if one of the following is true:

1) $a \equiv 1 \pmod p$
2) $a \equiv -1 \pmod p$
3) $a^2 \equiv -1 \pmod p$
4) $a^2 \equiv 1 \pmod p$

The values of a that satisfy are the non-trivial solutions

b) This is false?

As given in lecture notes,

there are 8 square roots of 1 in

$\mathbb{Z}/561\mathbb{Z}$, which 188 is one of them.

However, $\gcd(a-1, p) = \gcd(187, 561)$

$= 187$, which is not prime.

Same can be said for 560:

$\gcd(559, 561) = 1$ not prime