Math 116 HW3 Jun Ryu

1) a) Alice's public key:

$$A \equiv g^a \equiv 2^{947} \pmod{1373}$$
$$\equiv \boxed{177} \pmod{1373} \text{ (using Sage)}$$

b) $c_1 \equiv g^k \equiv 2^{877} \equiv 719 \pmod{1373}$

$c_2 \equiv mB^k \equiv 583 \cdot 469^{877} \equiv 623 \pmod{1373}$

Thus, Alice sends (c_1, c_2) or $\boxed{(719, 623)}$ to Bob.

c) $m \equiv c_2 \cdot (c_1)^{-a} \equiv 1325 \cdot (661)^{-299}$

$\equiv 332 \pmod{1373}$

Thus, the plaintext is $m = \boxed{332}$.

3) a) We check

$$\lim_{x \to \infty} \frac{x^2 + \sqrt{x}}{x^2} = \lim_{x \to \infty} 1 + x^{-3/2} = 1$$

Thus, a finite limit exists $\Rightarrow x^2 + \sqrt{x} = O(x^2)$ ✓

b) We check

$$\lim_{x\to\infty} \frac{5+6x^2-37x^5}{x^5} = \lim_{x\to\infty} \frac{5}{x^5} + \frac{6}{x^3} - 37 = -37$$

Thus, a finite limit exists $\Rightarrow 5+6x^2-37x^5 = O(x^5)$ ✓

c) We check

$$\lim_{k\to\infty} \frac{k^{300}}{2^k} = 0$$

Thus, a finite limit exists $\Rightarrow k^{300} = O(2^k)$ ✓

d) We check

$$\lim_{k\to\infty} \frac{(\ln k)^{375}}{k^{0.001}} = 0$$

Thus, a finite limit exists $\Rightarrow (\ln k)^{375} = O(k^{0.001})$ ✓

e) We check

$$\lim_{k\to\infty} \frac{k^2 2^k}{e^{2k}} = 0$$

Thus, a finite limit exists $\rightarrow k^2 2^k = O(e^{2k})$ ✓

f) We check

$$\lim_{N\to\infty} \frac{N^{10} 2^N}{e^N} = 0$$

Thus, a finite limit exists $\Rightarrow N^{10} 2^N = O(e^N)$ ✓

4) a) $11^x = 21$ in $\mathbb{F}_{71}$

11 has order 70 in $\mathbb{F}_{71}$ $(11^{70} \equiv 1 \pmod{71})$

So, let $n = 1 + \lfloor \sqrt{N} \rfloor = 1 + \lfloor \sqrt{70} \rfloor = 9$

Then, list 1:

$$
\begin{array}{ccccccccc}
g^0 & g^1 & g^2 & g^3 & g^4 & g^5 & g^6 & \cdots \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
1 & 11 & 121 & 550 & 583 & 165 & 253 & \\
 & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
 & & 50 & 53 & 15 & 23 & 40 &
\end{array}
$$

list 2: (we note that $g^{-n} \equiv 11^{-9} \equiv 7 \pmod{71}$)

$$
\begin{array}{cccccc}
h & hg^{-9} & hg^{-18} & hg^{-27} & hg^{-36} & \cdots \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
21 & 147 & 35 & 245 & 224 & \\
 & \downarrow & & \downarrow & \downarrow & \\
 & 5 & & 32 & 11 &
\end{array}
$$

$\Rightarrow g^1 = hg^{-36} \Rightarrow h = g^{37}$

$\Rightarrow \boxed{x = 37}$

b) $156^x = 116$ in $\mathbb{F}_{593}$

156 has order 148 in $\mathbb{F}_{593}$. ($156^{148} \equiv 1 \pmod{593}$)

So, let $n = 1 + \lfloor \sqrt{N} \rfloor = 1 + \lfloor \sqrt{148} \rfloor = 13$

List 1:

g^0	1
g^1	156
g^2	23
g^3	30
g^4	529
g^5	97
g^6	307
$\boxed{g^7}$	$\boxed{452}$

List 2:

hg^{-13}	58
hg^{-26}	29
hg^{-39}	311
$\boxed{hg^{-52}}$	$\boxed{452}$

$\Rightarrow g^7 = hg^{-52} \Rightarrow h = g^{59} \Rightarrow \boxed{x = 59}$

5) a) $x \equiv 3 \pmod 7$ and $x \equiv 4 \pmod 9$

$x = 3 + 7y$, $y \in \mathbb{Z}$

$3 + 7y \equiv 4 \pmod 9$

$7y \equiv 1 \pmod 9 \Rightarrow y \equiv 4$

$x \equiv 3 + 7(4) = \boxed{31} \pmod{63}$

b) $x \equiv 137 \pmod{423}$ and $x \equiv 87 \pmod{191}$

$x = 137 + 423y,\ y \in \mathbb{Z}$

$137 + 423y \equiv 87 \pmod{191}$

$423y \equiv 141 \pmod{191}$

Inverse of 423 modulo 191:

$423z \equiv 1 \pmod{191}$

$z \equiv 14$

$y \equiv 14 \cdot 141 \pmod{191}$

$y = 64$

$x \equiv 137 + 423 \cdot 64 = \boxed{27209} \pmod{80793}$

c) $x \equiv 5 \pmod 9$, $x \equiv 6 \pmod{10}$, $x \equiv 7 \pmod{11}$

$x = 5 + 9y,\ y \in \mathbb{Z}$

$5 + 9y \equiv 6 \pmod{10}$

$9y \equiv 1 \pmod{10}$

$y = 9$

$x = 5 + 9(9) = 86$

Now,

$$x = 86 + 90z \quad , z \in \mathbb{Z}$$

$$86 + 90z \equiv 7 \pmod{11}$$

$$90z \equiv 9 \pmod{11}$$

Inverse of 90 modulo 11:

$$90w \equiv 1 \pmod{11}$$

$$w \equiv 6$$

$$z \equiv 6 \cdot 9 \pmod{11}$$

$$z = 10$$

$$x \equiv 86 + 90(10) = \boxed{986} \pmod{990}$$