Daren Liu, Blue   Ryan Summers, Red

NT-18) $17^{53} (\text{mod } 97)$ $b=17$ $n=53$ $m=97$

$53 = [\overset{5}{1}\ \overset{4}{1}\ \overset{3}{0}\ \overset{2}{1}\ \overset{1}{0}\ \overset{0}{1}]$

i	b	s	a
—	—	—	1
0	17	1	17
1	95	0	17
2	4	1	68
3	16	0	68
4	62	1	45
5	61	1	29

$17^{53} \equiv 29 (\text{mod } 97)$

RSA-1) $p=7$ $q=97$ $e=257$

$n = pq = 679$ $\theta(n) = (96)(6) = 576$

$d = 257^{-1} (\text{mod } 576) = 65$

$\underline{576} = \underline{257} \cdot 2 + \underline{62}$ $1 = \underline{9} - \underline{8} \cdot 1$

$\underline{257} = \underline{62} \cdot 4 + \underline{9}$ $1 = 9 - (\underline{62} - \underline{9} \cdot 6) = \underline{9} \cdot 7 - \underline{62}$

$\underline{62} = \underline{9} \cdot 6 + \underline{8}$ $1 = 7(\underline{257} - \underline{62} \cdot 4) - \underline{62}$

$\underline{9} = \underline{8} \cdot 1 + \underline{1}$ $= -29 \cdot \underline{62} + 7 \cdot \underline{257}$

$= -29(\underline{576} - \underline{257} \cdot 2) + 7 \cdot \underline{257}$

$= 65 \cdot \underline{257} - 29 \cdot \underline{576}$

$146^{d} (\mathrm{mod}\ n) = 146^{65} (\mathrm{mod}\ 679)$

$65 = \overset{6}{1}\overset{5}{0}\overset{4}{0}\overset{3}{0}\overset{2}{0}\overset{1}{0}\overset{0}{1}$

1

i	b	s	a
0	146	1	146
1	267	0	146
2	673	0	146
3	36	0	146
4	617	0	146
5	449	0	146
6	617	1	454

$$146^{65} \equiv 454 (\mathrm{mod}\ 679)$$

$a = 454/26 = 17$

$b = 454 \% 26 = 12$

$C \equiv 17p + 12 (\mathrm{mod}\ 26)$

$P \equiv a'C + b' (\mathrm{mod}\ 26)$

$C - 12 = 17P (\mathrm{mod}\ 26)$

$P = 17^{-1}(C-12) = 23(C-12)$

$\underline{26} = \underline{17} \cdot 1 + \underline{9}$ $\qquad$ $\underline{1} = \underline{9} - \underline{8}$

$\underline{17} = \underline{9} \cdot 1 + \underline{8}$ $\qquad$ $\underline{1} = \underline{9} - (\underline{17} - \underline{9}) = 2 \cdot \underline{9} - \underline{17}$

$\underline{9} = \underline{8} \cdot 1 + \underline{1}$ $\qquad$ $\underline{1} = 2(\underline{26} - \underline{17}) - \underline{17} = 2 \cdot \underline{26} - 3 \cdot \underline{17}$

$23 \cdot \underline{17} \pmod{26}$

CT	$23(c-12) \pmod{26}$	PT
P	$23(3) \pmod{26} = 17$	R
B	$23(1-12) \pmod{26} = 7$	H
E	$23(4-12) \pmod{26} = 24$	Y
X	$23(23-12) \pmod{26} = 19$	T
B		H
I	$23(8-12) \pmod{26} = 12$	M

$C \equiv aP + b \pmod{26}$ $a = 11, b = 21$

$X = 26(11) + 21 = 307$

$x^e \pmod{n}$

$307^{19} \pmod{681}$

$19 = [1\ 0\ 0\ 1\ 1]$

1

i	b	s	q
0	307	1	307
1	271	1	115
2	574	0	115
3	553	0	115
4	40	1	514

514

LM-4) 9A3F

RSA-2) n, e, p

$n = pq \quad q = \frac{n}{p}$

$q = 3146....$

$\Theta(n) = (p-1)(q-1) = 2314...$

$d = e^{-1} \bmod \Theta(n) = 1071$

RSA-3) Key = Mod(b1AESK1, n) ^ d = 43690

PT = fresh freaken crawdad. Whats my middle name

RSA-4) Number I gave partner for 51913: 1715...

Number I gave partner for 51914: 1451...