18.310A Problem Set 5

Rishad Rahman

1. We need to find $7^{-1} \bmod 16 \cdot 30$.

a	b	b'
480	7	$4 = 480 - 68(7)$
7	4	$1 = 2(4) - 7 = 2(480) - 137(7)$

Therefore $7^{-1} \equiv -137 \equiv 343 \mod 16 \cdot 30$ so our decoding function is $s^{343} \bmod 527$.

2. a) Consider $240^2 \cdot 247^2 \cdot 253^2 \equiv 2^4 \cdot 5^6 \cdot 7^2 \cdot 13^2 \bmod 57509 \Rightarrow (240 \cdot 247 \cdot 253)^2 \equiv (2^2 \cdot 5^3 \cdot 7 \cdot 13)^2 \bmod 57509 \Rightarrow (240 \cdot 247 \cdot 253 - 2^2 \cdot 5^3 \cdot 7 \cdot 13)(240 \cdot 247 \cdot 253 + 2^2 \cdot 5^3 \cdot 7 \cdot 13) \equiv 0 \bmod 57509$. But notice $240 \cdot 247 \cdot 253 - 2^2 \cdot 5^3 \cdot 7 \cdot 13 = 14952340 \equiv 0 \mod 57509$ so this does not give us a factor.

b) Consider $241^2 \cdot 254^2 \equiv 2^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \bmod 57509 \Rightarrow (241 \cdot 254)^2 \equiv (2 \cdot 7 \cdot 11 \cdot 13)^2 \bmod 57509 \Rightarrow (241 \cdot 254 + 2 \cdot 7 \cdot 11 \cdot 13)(241 \cdot 254 - 2 \cdot 7 \cdot 11 \cdot 13) \equiv 0 \bmod 57509$. We can check $241 \cdot 254 + 2 \cdot 7 \cdot 11 \cdot 13 = 63216 \not\equiv 0 \bmod 57509$ and $241 \cdot 254 - 2 \cdot 7 \cdot 11 \cdot 13 = 59212 \not\equiv 0 \bmod 57509$. So to find our factor, $\gcd(59212, 57509) = \gcd(57509, 1703) = \gcd(1703, 1310) = \gcd(1310, 393) = \gcd(393, 131) = 131$.

3. Eve can find the common prime factor to N_A and N_B by Euclid's Algorithm which would then give her the other primes as well by division which would allow her to find the private keys and thus be able to decode their messages.

4. Note $5^{12} \equiv 1 \bmod 13$ by FLT. So we want to find $7^{11} \bmod 12$. But $7^{11} \equiv 7 \cdot (7^2)^5 \equiv 7 \cdot (49)^5 \equiv 7 \bmod 12$. So $5^{7^{11}} \equiv 5^7 \equiv 5 \cdot (5^2)^3 \equiv -5 \equiv 8 \bmod 13$.

5. a) Take a group of k elements of a mapping. The probability they form a cycle is $\frac{(k-1)! n^{n-k}}{n^n} = \frac{(k-1)!}{n^k}$. Since there are total of n^n functions, $(k-1)!$ cycles of k elements (since $f(m_j)$ has $k - j$ possible choices), and n^{n-k} possible choices for the elements not in our selected k. Therefore by linearity of expectation the expected number of k cycles is $\frac{\binom{n}{k}(k-1)!}{n^k}$.

b) The expected number of cycles is $\displaystyle\sum_{k=1}^{n} \frac{\binom{n}{k}(k-1)!}{n^k} = \sum_{k=1}^{n} \frac{1}{k} \cdot \frac{n!}{(n-k)! \cdot n^k} < \sum_{k=1}^{n} \frac{1}{k} \sim O(\log n)$ so the expected number of cycles is less than a function which is $O(\log n)$ which implies it is also $O(\log n)$.

c) By Markov's Inequality, $\mathbb{P}(X \geq 100\sqrt{n}) \leq \frac{\mu}{100\sqrt{n}} \leq \frac{\log n}{100\sqrt{n}}$ and since $\sqrt{n}$ dominates $\log n$ for large n (we have $n \geq 10^4$), the probability that we have larger than $100\sqrt{n}$ cycles turns very small.