MATH 173A Project

Megan Chu

07/27/18

Problem Solving (Latex) 3.10 and 3.19

Ex.3.10. A decryption exponent for an RSA public key (N, e) is an integer d with the property that $a^{de} \equiv a(modN)$ for all integers a that are relatively prime to N.

a) Suppose that Eve has a magic box that creates decryption exponents for (N, e) for a fixed modulus N and for a large number of different encryption exponents e. Explain how Eve can use her magic box to try to factor N.

Solution: Eve knows a large number of different encryption exponents, which we will denote as $e_1, e_2, ..., e_k$. Using the magic box, Eve can obtain all decryption exponents for the set of encryption exponents, which we will denote as $d_1, d_2, ..., d_k$, and where d_n is the decryption exponent for the RSA public key (N, e_n) where $n \in \{1, 2, ..., k\}$.

In general, N can be factored into primes $p_1p_2...p_r$, such that $N = p_1p_2...p_r$. Eve also knows that

$$a^{de} \equiv a(\text{mod } N) \equiv a(\text{mod } p_1) \equiv a(\text{mod } p_2) \equiv ... \equiv a(\text{mod } p_r),$$

since N is a multiple of any one of the primes in the set $p_1, p_2, ..., p_r$.

Then, $de \equiv 1(\text{mod } (p_1 - 1)) \equiv 1(\text{mod } (p_2 - 1) \equiv ... \equiv 1(\text{mod } (p_r - 1))$ must be true, so that the following statements can also hold true.

$$\begin{gathered} a^{de} \equiv a^{k(p_1-1)+1} \equiv (a^{p_1-1})^k a^1 \equiv 1^k a \equiv a(\text{mod } p_1), \\ a^{de} \equiv a^{k(p_2-1)+1} \equiv (a^{p_2-1})^k a^1 \equiv 1^k a \equiv a(\text{mod } p_2), \\ ..., \\ a^{de} \equiv a^{k(p_r-1)+1} \equiv (a^{p_r-1})^k a^1 \equiv 1^k a \equiv a(\text{mod } p_r). \end{gathered}$$

This also implies that $de \equiv 1(\text{mod } (p_1 - 1)(p_2 - 1)...(p_r - 1))$;

equivalently, $de - 1 \equiv 0(\text{mod } \phi(N))$;

equivalently, $\phi(N)|de - 1$.

Since we know that the RSA public key cryptosystem involves N as a product of 2 primes, we can say $N = pq$ for primes p and q. Eve can now compute the following value: $b = gcd(d_1e_1 - 1, d_2e_2 - 1, ..., d_ke_k - 1)$, with confidence that b is a factor of $\phi(N) = (p - 1)(q - 1)$. Note that we assume we have enough encryption/decryption exponent pairs such that b will be a small value less than $(p - 1)(q - 1)$.

Remark 3.11 from the textbook tells us we can expand $\phi(N)$ like so:

$$\begin{aligned} \phi(N) &= (p - 1)(q - 1) \\ &= pq - p - q + 1 \\ &= N - (p + q) + 1. \end{aligned}$$

Since Eve knows the value of N, if she can find out the value of $p+q$, she can solve for the value $(p-1)(q-1)$. Furthermore, if Eve knows the values of $p+q$ and $N = pq$, she can use the quadratic formula to solve the equation

$$x^2 - (p+q)x + pq = (x-p)(x-q) = 0 \tag{3.10.1}$$

for its roots p and q.

Eve can try random values of $p+q$ to see if they result in (3.10.1) having integer factors. This method can be further simplified since Eve knows b is a factor of $(p-1)(q-1)$. In other words, $bi = (p-1)(q-1)$ for some $i \in \mathbb{Z}$. We also see that

$$\begin{aligned}(p-1)(q-1) &= N - (p+q) + 1 \\ &\Leftrightarrow (p+q) = N + 1 - (p-1)(q-1) \\ &\Leftrightarrow (p+q) = N + 1 - bi \text{ for some } i \in \mathbb{Z}.\end{aligned}$$

Thus, Eve can try increasing integers for i starting from 1, solve for $(p+q)$, and try to factor (3.10.1). Furthermore, Eve can estimate i since

$$\begin{aligned}bi =&(p-1)(q-1) \\ &\Rightarrow bi < (p)(q) \\ &\Rightarrow bi < N \\ &\Rightarrow i < \frac{N}{b}.\end{aligned}$$

Thus, Eve only has to test decreasing values of i starting from the first integer less than $\frac{N}{b}$ and stopping at $i = 1$. Once she finds a value for i giving a $(p+q)$ that allows for factorization of (3.10.1) into integer roots, she can use the quadratic formula to find p and q; hence, factoring N.

b) Let $N = 38749709$. Eve's magic box tells her that the encryption exponent $e = 10988423$ has decryption exponent $d = 16784693$ and that the encryption exponent $e = 25910155$ has decryption exponent $d = 11514115$. Use this information to factor N.

Solution: Following (a), we calculate b and i

$$\begin{aligned} b =& gcd(d_1 e_1 - 1, d_2 e_2 - 1) \\ &= gcd(16784693 \cdot 10988423 - 1, 11514115 \cdot 25910155 - 1) \\ &= gcd(184437306609138, 298332504337824) \\ &= 19368558, \text{ using the wolframalpha gcd calculator} \end{aligned}$$

$$i < \frac{N}{b} < \frac{38749709}{19368558} < 2.00065017747 \Rightarrow i \approx 2$$

Thus, we try i = 2:

$$p + q = N + 1 - b \cdot i = 38749709 + 1 - 19368558 \cdot 2 = 12594$$

Then, $a' = 1, b' = 12594, c' = N = 38749709$, and $x^2 - 12594x + 38749709 = 0$ has solutions

$$x = \frac{b' \pm \sqrt{b'^2 - 4a'c'}}{2a'} = \frac{12594 \pm \sqrt{3610000}}{2} = 5347 \text{ or } 7247$$

Thus, $\boxed{N = 5347 \cdot 7247}$.

c) Let $N = 225022969$. Eve's magic box tells her the following three encryption/decryption pairs for N:
(70583995, 4911157), (173111957, 7346999), (180311381, 29597249).
Use this information to factor N.

Solution: We calculate b and i

$$\begin{aligned} b =& gcd(d_1e_1 - 1, d_2e_2 - 1, d_3e_3 - 1) \\ &= gcd(4911157 \cdot 70583995 - 1, 7346999 \cdot 173111957 - 1, 29597249 \cdot 180311381 - 1) \\ &= gcd(346649081132214, 1271853374967042, 5336720840990868) \\ &= 37498566, \text{ using the wolframalpha gcd calculator} \end{aligned}$$

$$i < \frac{N}{b} < \frac{225022969}{37498566} < 6.00084197886 \Rightarrow i \approx 6$$

To avoid trying many values of i by hand, we use a computer program to do such calculations and we see that i = 6 indeed gives integer solutions. When i = 6,

$$p + q = N + 1 - b \cdot i = 225022969 + 1 - 37498566 \cdot 6 = 31574$$

Then, $a' = 1, b' = 31574, c' = N = 225022969$, and $x^2 - 31574x + 225022969 = 0$ has solutions

$$x = \frac{b' \pm \sqrt{b'^2 - 4a'c'}}{2a'} = \frac{31574 \pm \sqrt{96825600}}{2} = 10867 \text{ or } 20707$$

Thus, $\boxed{N = 10867 \cdot 20707}$.

d) Let $N = 1291233941$. Eve's magic box tells her the following three encryption/decryption pairs for N:
(1103927639, 76923209), (1022313977, 106791263), (387632407, 7764043). Use this information to factor N.

Solution: We calculate b and i

$$\begin{aligned} b =& gcd(d_1e_1 - 1, d_2e_2 - 1, d_3e_3 - 1) \\ &= gcd(76923209 \cdot 1103927639 - 1, 106791263 \cdot 1022313977 - 1, 7764043 \cdot 387632407 - 1) \\ &= gcd(84917656495673550, 109174200786382950, 3009594676141500) \\ &= 129112350, \text{ using the wolframalpha gcd calculator} \end{aligned}$$

$$i < \frac{N}{b} < \frac{1291233941}{129112350} < 10.0008553868 \Rightarrow i \approx 10$$

To avoid trying many values of i by hand, we use a computer program to do such calculations and we see that i = 10 indeed gives integer solutions. When i = 10,

$$p + q = N + 1 - b \cdot i = 1291233941 + 1 - 129112350 \cdot 10 = 110442$$

Then, $a' = 1, b' = 110442, c' = N = 1291233941$, and $x^2 - 110442x + 1291233941 = 0$ has solutions

$$x = \frac{b' \pm \sqrt{b'^2 - 4a'c'}}{2a'} = \frac{110442 \pm \sqrt{7032499600}}{2} = 13291 \text{ or } 97151$$

Thus, $\boxed{N = 13291 \cdot 97151}$.

Ex.3.19. We noted in Sect. 3.4 that it really makes no sense to say that the number n has probability $1/\ln(n)$ of being prime. Any particular number that you choose either will be prime or will not be prime; there are no numbers that are 35% prime and 65% composite! In this exercise you will prove a result that gives a more sensible meaning to the statement that a number has a certain probability of being prime. You may use the prime number theorem (Theorem 3.21) for this problem.

a) Fix a (large) number N and suppose that Bob chooses a random number n in the interval $\frac{1}{2}N \le n \le \frac{3}{2}N$. If he repeats this process many times, prove that approximately $1/\ln(N)$ of his numbers will be prime. More precisely, define

$$P(N) = \frac{\text{number of primes between} \frac{1}{2}N \text{ and } \frac{3}{2}N}{\text{number of integers between} \frac{1}{2}N \text{ and } \frac{3}{2}N} (\textit{inclusive})$$
$$= \left[\begin{array}{c}\text{Probability that an integer } n \text{ in the} \\ \text{interval } \frac{1}{2}N \le n \le \frac{3}{2}N \text{ is a prime number}\end{array} \right],$$

and prove that

$$\lim_{N\to\infty} \frac{P(N)}{1/\ln(N)} = 1.$$

This shows that if N is large, then $P(N)$ is approximately $1/\ln(N)$.

<u>*Solution:*</u> Supposing that N is divisible by 2, we see that the number of integers between $\frac{1}{2}N$ and $\frac{3}{2}N$ is equal to $\frac{3}{2}N - \frac{1}{2}N + 1 = \frac{2}{2}N + 1 = N + 1$. Even if N is not divisible by 2, the number of integers between $\frac{1}{2}N$ and $\frac{3}{2}N$ is still at least $N - 1$. Regardless of the divisibility of N, since N approaches ∞ in the limit we want to prove, and since the number of integers between $\frac{1}{2}N$ and $\frac{3}{2}N$ has the value of $N+$ "some constant", we can simplify the number of integers between $\frac{1}{2}N$ and $\frac{3}{2}N$ to just $\boxed{N}$ without affecting the final result of the limit.

Section 3.4.1 in the textbook says that by definition,
$\pi(X) = (\#\text{ of primes } p \text{ satisfying } 2 \le p \le X)$. Thus,

$$\pi(\frac{3}{2}N) = (\#\text{ of primes between 2 and } \frac{3}{2}N)$$

$$\pi(\frac{1}{2}N) = (\#\text{ of primes between 2 and } \frac{1}{2}N)$$

It follows that

$$\#\text{ of primes between } \frac{1}{2}N \text{ and } \frac{3}{2}N = \boxed{\pi(\tfrac{3}{2}N) - \pi(\tfrac{1}{2}N)}$$

Thus, as $N \to \infty$, $P(N) \to \frac{\pi(\frac{3}{2}N) - \pi(\frac{1}{2}N)}{N}$, and we have,

$$\lim_{N\to\infty} \frac{P(N)}{1/\ln(N)} = \lim_{N\to\infty} \frac{\frac{\pi(\frac{3}{2}N) - \pi(\frac{1}{2}N)}{N}}{1/\ln(N)} = \lim_{N\to\infty} \frac{\pi(\frac{3}{2}N) - \pi(\frac{1}{2}N)}{N/\ln(N)}$$

Theorem 3.21 (The Prime Number Theorem) from the textbook tells us that $\lim_{N\to\infty} \frac{\pi(X)}{X/\ln(N)} = 1$. Hence, we can replace the terms $\pi(\frac{3}{2}N)$ and $\pi(\frac{1}{2}N)$ with $\frac{3}{2}N/\ln(\frac{3}{2}N)$ and $\frac{1}{2}N/\ln(\frac{1}{2}N)$, respectively, without affecting the final result of the limit. Thus,

$$\begin{aligned}
\lim_{N\to\infty} \frac{\pi(\frac{3}{2}N) - \pi(\frac{1}{2}N)}{N/\ln(N)} &= \lim_{N\to\infty} \frac{\frac{3}{2}N/\ln(\frac{3}{2}N) - \frac{1}{2}N/\ln(\frac{1}{2}N)}{N/\ln(N)} \\
&= \lim_{N\to\infty} \frac{\frac{3}{2}/\ln(\frac{3}{2}N) - \frac{1}{2}/\ln(\frac{1}{2}N)}{1/\ln(N)} \\
&= \lim_{N\to\infty} \frac{\frac{3}{2}/\ln(\frac{3}{2}N)}{1/\ln(N)} - \frac{\frac{1}{2}/\ln(\frac{1}{2}N)}{1/\ln(N)} \\
&= \lim_{N\to\infty} \frac{\frac{3}{2}\ln(N)}{\ln(\frac{3}{2}N)} - \frac{\frac{1}{2}\ln(N)}{\ln(\frac{1}{2}N)} \\
&= \lim_{N\to\infty} \frac{3\ln(N)}{2\ln(\frac{3}{2}N)} - \frac{1\ln(N)}{2\ln(\frac{1}{2}N)}
\end{aligned}$$

Clearly, as $N \to \infty$ the values of $\ln(N)$, $\ln(\frac{3}{2}N)$, and $\ln(\frac{1}{2}N)$ plateau, since all three funtions are $O(\ln(N))$ and have logarithmic growth. In other words, as $N \to \infty$, the values of $\ln(N)$, $\ln(\frac{3}{2}N)$, and $\ln(\frac{1}{2}N)$ will converge/approach each other. Thus, we can cancel out these terms without affecting the final result of the limit.

$$\begin{aligned}
\lim_{N\to\infty} \frac{3\ln(N)}{2\ln(\frac{3}{2}N)} - \frac{1\ln(N)}{2\ln(\frac{1}{2}N)} &= \lim_{N\to\infty} \frac{3}{2} - \frac{1}{2} \\
&= \frac{3}{2} - \frac{1}{2} \\
&= \frac{2}{2} \\
&= 1
\end{aligned}$$

We have shown $\lim_{N\to\infty} \frac{P(N)}{1/\ln(N)} = 1$. $\square$

b) More generally, fix two numbers c_1 and c_2 satisfying $c_2 > c_1 > 0$. Bob chooses random numbers n in the interval $c_1 N \leq n \leq c_2 N$. Keeping c_1 and c_2 fixed, let

$$P(c_1, c_2; N) = \left[\begin{smallmatrix}\text{Probability that an integer } n \text{ in the inter-}\\ \text{val } c_1 N \leq n \leq c_2 N \text{ is a prime number}\end{smallmatrix}\right].$$

In the following formula, fill in the box with a simple function of N so that the statement is true:

$$\lim_{N\to\infty} \frac{P(c_1, c_2; N)}{\boxed{}} = 1.$$

Solution: From part (a), we proved that if $c_2 = \frac{3}{2}$ and $c_1 = \frac{1}{2}$, then, $\lim_{N\to\infty} \frac{P(c_1,c_2;N)}{1/\ln(N)} = \frac{3}{2} - \frac{1}{2} = c_2 - c_1 = 1$. Seeing that

$$\lim_{N\to\infty} \frac{P(c_1, c_2; N)}{1/\ln(N)} = c_2 - c_1 \tag{3.19.1}$$

and using the knowledge that $\frac{c_2 - c_1}{c_2 - c_1} = 1$, we divide both sides of (3.19.1) by $c_2 - c_1$.

$$\begin{aligned}
&\frac{1}{c_2 - c_1} \lim_{N\to\infty} \frac{P(c_1, c_2; N)}{1/\ln(N)} = \frac{c_2 - c_1}{c_2 - c_1} = 1 \\
\Leftrightarrow &\lim_{N\to\infty} \left(\frac{1}{c_2 - c_1}\right) \frac{P(c_1, c_2; N)}{1/\ln(N)} = 1 \\
\Leftrightarrow &\lim_{N\to\infty} \frac{P(c_1, c_2; N)}{\boxed{(c_2 - c_1)/\ln(N)}} = 1
\end{aligned}$$

Thus, $\boxed{(c_2 - c_1)/\ln(N)}$ correctly fills in the box so that $\lim_{N\to\infty} \frac{P(c_1,c_2;N)}{\boxed{}} = 1$ is true.