MATH 470.200/501
Examination 2 Solutions
November 3, 2011

1. Alice and Bob are using RSA to communicate.

   (a) Alice's encryption key is $(n_1, e_1) = (187, 7)$. Alice wants to encode the plaintext '10' to send to Bob. What is the ciphertext that she sends?

   (b) On another occasion, you intercept the ciphertext '5' sent to Alice. Find Alice's decryption key and write down the expression that yields the plaintext. (You do not need to calculate the plaintext completely.)

   (c) Suppose that Bob's encryption key is $(n_2, e_2) = (989, 12)$, and suppose that we have discovered that $\phi(989) = 924$. Use this information to factor 989.

   Solution: (a) The ciphertext is $c \equiv 10^7 \pmod{187}$. We reduce this modulo 187 and find $\boxed{c \equiv 175 \pmod{187}.}$

   (b) The decryption exponent d is the multiplicative inverse of $e = 7$ modulo $\phi(187)$. We factor $187 = 11 \cdot 17$, so then $\phi(187) = 10 \cdot 16 = 160$. Therefore $d \equiv \frac{1}{7} \equiv 23 \pmod{160}$. There fore the plaintext is $\boxed{m \equiv 5^{23} \pmod{187}.}$ This further reduces to 180, but it was not necessary to calculate that far.

   (c) If $n = 989 = pq$, we know that the quadratic polynomial $x^2 - (n - \phi(n) + 1)x + n = (x - p)(x - q)$. So we find the roots of $x^2 - 66x + 989 = 0$: by the quadratic formula,

$$x = \frac{66 \pm \sqrt{400}}{2} = \frac{66 \pm 20}{2} = 23,\ 43.$$

   Therefore, $\boxed{989 = 23 \cdot 43.}$

2. The following congruences hold:

$$789^{495} \equiv 8154 \pmod{15841} \qquad 789^{990} \equiv 3039 \pmod{15841} \tag{1}$$
$$789^{1980} \equiv 218 \pmod{15841} \qquad 789^{3960} \equiv 1 \pmod{15841} \tag{2}$$
$$789^{7920} \equiv 1 \pmod{15841} \qquad 789^{15840} \equiv 1 \pmod{15841} \tag{3}$$

$$123^{1625} \equiv 4852 \pmod{13001} \qquad 123^{3250} \equiv 10094 \pmod{13001} \tag{4}$$
$$123^{6500} \equiv 13000 \pmod{13001} \qquad 123^{13000} \equiv 1 \pmod{13001} \tag{5}$$

   (a) Using the data in lines (1)–(3) above, apply the Miller-Rabin Primality Test to $n = 15841$. What can you conclude about 15841? Explain.

   (b) Using the data in lines (4)–(5) above, apply the Miller-Rabin Primality Test to $n = 13001$. What can you conclude about 13001? Explain.

   Solution: (a) $n - 1 = 15840 = 2^5 \cdot 495$. We apply the Miller-Rabin Test with $a = 789$. From the given data,

$$\begin{aligned}
b_0 &\equiv 789^{495} \equiv 8154 && \not\equiv \pm 1 && \pmod{15841},\\
b_1 &\equiv b_0^2 \equiv 789^{990} \equiv 3039 && \not\equiv -1 && \pmod{15841},\\
b_2 &\equiv b_1^2 \equiv 789^{1980} \equiv 218 && \not\equiv -1 && \pmod{15841},\\
b_3 &\equiv b_2^2 \equiv 789^{3960} \equiv 1 && \not\equiv -1 && \pmod{15841},\\
b_4 &\equiv b_3^2 \equiv 789^{7920} \equiv 1 && \not\equiv -1 && \pmod{15841}.
\end{aligned}$$

Therefore, $\boxed{n = 15841 \text{ must be composite.}}$

(b) $n - 1 = 13000 = 2^3 \cdot 1625$. We apply the Miller-Rabin Test with $a = 123$. From the given data,

$$\begin{aligned} b_0 &\equiv 123^{1625} \equiv 4852 && \not\equiv \pm 1 && \pmod{13001}, \\ b_1 &\equiv b_0^2 \equiv 123^{3250} \equiv 10094 && \not\equiv -1 && \pmod{13001}, \\ b_2 &\equiv b_1^2 \equiv 123^{6500} \equiv 13000 && \equiv -1 && \pmod{13001}. \end{aligned}$$

At this point, we stop since when we get to b_2 we obtain -1 modulo $n = 13001$. Therefore the Miller-Rabin Test is $\boxed{\text{inconclusive}}$ or $\boxed{n = 13001 \text{ is 'probably prime'.}}$

3. Suppose that $n = 1643$ is being used for RSA encryption, and suppose that we have discovered that the encryption exponent is $e = 29$ and that the decryption exponent is $d = 269$. Suppose further that the following congruences hold:

$$\begin{aligned} 2^{975} &\equiv 1613 \pmod{1643} & 3^{975} &\equiv 712 \pmod{1643} \\ 5^{975} &\equiv 931 \pmod{1643} & 6^{975} &\equiv 1642 \pmod{1643}. \end{aligned}$$

Use the Universal Exponent Factorization Method to factor 1643. Show your work.

Solution: Because $e = 29$ and $d = 269$ are encryption and decryption exponents for RSA, we know that $r = de - 1 = 7800$ is a universal exponent modulo $n = 1643$. Now $7800 = 2^3 \cdot 975$, so the given data contains some potential first steps in the Universal Exponent Factorization Method. So we try the first one, with $a = 2$, and we have

$$\begin{aligned} b_0 &\equiv 2^{975} \equiv 1613 && \not\equiv \pm 1 && \pmod{1643}, \\ b_1 &\equiv b_0^2 \equiv 900 && \not\equiv \pm 1 && \pmod{1643}, \\ b_2 &\equiv b_1^2 \equiv 1 && \equiv 1 && \pmod{1643}. \end{aligned}$$

Since $b_2 \equiv 1 \pmod{1643}$ but $b_1 \not\equiv \pm 1 \pmod{1643}$, we conclude that $b_1 - 1 = 900 - 1 = 899$ must share a nontrivial factor with 1643. So we use the Euclidean Algorithm to compute $\gcd(899, 1643)$:

$$\begin{aligned} 1643 &= 899 + 744, \\ 899 &= 744 + 155, \\ 744 &= 4 \cdot 155 + 124, \\ 155 &= 124 + 31, \\ 124 &= 4 \cdot 31 + 0. \end{aligned}$$

Therefore $\gcd(899, 1643) = 31$ and 31 divides 1643. Dividing 1643 by 31, we see that $\boxed{1643 = 31 \cdot 53.}$

4. Let $n = 7991$. We know that 7991 is the product of two distinct primes. Suppose in carrying out the quadratic sieve that you have found that

$$\begin{aligned} 75^2 - n &= -2366, & 79^2 - n &= -1750, \\ 84^2 - n &= -935, & 94^2 - n &= 845, \\ 101^2 - n &= 2210, & 103^2 - n &= 2618. \end{aligned}$$

Use this information to factor 7991. Show your work.

Solution: We first factor each of the following numbers:

$$\begin{aligned} -2366 &= -2 \cdot 7 \cdot 13^2, & -1750 &= -2 \cdot 5^3 \cdot 7, \\ -935 &= -5 \cdot 11 \cdot 17, & 845 &= 5 \cdot 13^2, \\ 2210 &= 2 \cdot 5 \cdot 13 \cdot 17, & 2618 &= 2 \cdot 7 \cdot 11 \cdot 17. \end{aligned}$$

Therefore,

$$\begin{aligned} 75^2 &\equiv -2 \cdot 7 \cdot 13^2 \pmod{7991}, & 79^2 &\equiv -2 \cdot 5^3 \cdot 7 \pmod{7991}, \\ 84^2 &\equiv -5 \cdot 11 \cdot 17 \pmod{7991}, & 94^2 &\equiv 5 \cdot 13^2 \pmod{7991}, \\ 101^2 &\equiv 2 \cdot 5 \cdot 13 \cdot 17 \pmod{7991}, & 103^2 &\equiv 2 \cdot 7 \cdot 11 \cdot 17 \pmod{7991}. \end{aligned}$$

We now search for a subcollection of these congruences whose right-hand sides multiply together to give a perfect square. There are a few ways to do this, but here are two that work:

$$\begin{aligned} 75^2 \cdot 79^2 \cdot 94^2 &\equiv 2^2 \cdot 5^4 \cdot 7^2 \cdot 13^4 \pmod{7991}, \\ 79^2 \cdot 84^2 \cdot 103^2 &\equiv 2^2 \cdot 5^4 \cdot 7^2 \cdot 11^2 \cdot 17^2 \pmod{7991}. \end{aligned}$$

In the first case we take

$$\begin{aligned} x &\equiv 75 \cdot 79 \cdot 94 \equiv 556950 \equiv 5571 \pmod{7991}, \\ y &\equiv 2 \cdot 5^2 \cdot 7 \cdot 13 \equiv 59150 \equiv 3213 \pmod{7991}. \end{aligned}$$

We check easily that $x \not\equiv \pm y \pmod{7991}$, so we go ahead an compute $\gcd(x - y, 7991) = \gcd(2358, 7991)$:

$$\begin{aligned} 7991 &= 3 \cdot 2358 + 917, \\ 2358 &= 2 \cdot 917 + 524, \\ 917 &= 524 + 393, \\ 524 &= 393 + 131, \\ 393 &= 3 \cdot 131 + 0. \end{aligned}$$

Therefore $\gcd(2358, 7991) = 131$ is a factor of 7991, and by division the other is 61, yielding $\boxed{7991 = 61 \cdot 131.}$ Now in the second case (either one would suffice of course), we take

$$\begin{aligned} x &\equiv 79 \cdot 84 \cdot 103 \equiv 683508 \equiv 4273 \pmod{7991}, \\ y &\equiv 2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 17 \equiv 65450 \equiv 1522 \pmod{7991}. \end{aligned}$$

Again $x \not\equiv \pm y \pmod{7991}$, and we compute $\gcd(x - y, 7991) = \gcd(2751, 7991)$:

$$\begin{aligned} 7991 &= 2 \cdot 2751 + 2489, \\ 2751 &= 2489 + 262, \\ 2489 &= 9 \cdot 262 + 131, \\ 262 &= 2 \cdot 131 + 0. \end{aligned}$$

So $\gcd(2751, 7991) = 131$ and 131 divides 7991. Again we find that $\boxed{7991 = 61 \cdot 131.}$

5. Throughout this problem we work modulo $p = 19$, with chosen primitive root $\alpha = 3$.

   (a) Show that $L_3(5) = 4$.

   (b) Use the Pohlig-Hellman algorithm to find $L_3(2)$.

   Solution: (a) We check easily that $\boxed{3^4 \equiv 81 \equiv 5 \pmod{19}.}$

   (b) We first calculate that $p - 1 = 18 = 2 \cdot 3^2$. We let $x = L_3(2)$. First we calculate x modulo 2, so take $q = 2$. We need to find $x_0 \in \{0, 1\}$ so that $3^{9x_0} \equiv 2^9 \equiv 18 \pmod{19}$, which requires $x_0 = 1$. Therefore $x \equiv 1 \pmod{2}$.

   Now we calculate x modulo $3^2 = 9$, taking $q = 3$. We need to find $x_0 \in \{0, 1, 2\}$ so that $3^{6x_0} \equiv 2^6 \equiv 7 \pmod{19}$. We check that $x_0 = 1$. Then set $\beta_1 = 3^{-1} \cdot 2 \equiv 7 \pmod{19}$, and we need to find $x_1 \in \{0, 1, 2\}$ so that $3^{6x_1} \equiv \beta_1^{(p-1)/q^2} \equiv 7^2 \pmod{19}$. We check that $x_1 = 2$, and so $x \equiv 1 + 2 \cdot 3 \equiv 7 \pmod{9}$. So all together we need x to satisfy

$$x \equiv 1 \pmod{2}, \quad x \equiv 7 \pmod{9}.$$

   The Chinese Remainder Theorem states that this system has a unique solution modulo 18. By inspection $x \equiv 7 \pmod{18}$ satisfies both congruences, and so $\boxed{L_3(2) = 7.}$

6. Alice and Bob are again using RSA to communicate. They are using the same modulus n, so that Alice's public encryption key is (n, e_A) and Bob's is (n, e_B). Alice and Bob happen to have chosen e_A and e_B that are relatively prime.

   Now Charles wants to send the message m to both Alice and Bob. You may assume that $m < n$.

   (a) What does Charles send to Alice? What does he send to Bob?

   (b) Suppose that Eve intercepts both of these transmissions. Show how Eve can recover m without factoring n.

   Solution: (a) Charles sends $\boxed{c_A \equiv m^{e_A} \pmod{n}}$ to Alice and $\boxed{c_B \equiv m^{e_B} \pmod{n}}$ to Bob.

   (b) Eve intercepts c_A and c_B. Now since e_A and e_B are relatively prime ($gcd(e_A, e_B) = 1$), Eve can find s, $t \in \mathbb{Z}$ so that $se_A + te_B = 1$. Therefore, Eve calculates

$$\begin{aligned} c_A^s \cdot c_B^t &\equiv m^{se_A} \cdot m^{te_B} \pmod{n}, \\ &\equiv m^{se_A + te_B} \pmod{n}, \\ &\equiv m^1 \pmod{n}. \end{aligned}$$

   Therefore $\boxed{c_A^s \cdot c_B^t \equiv m \pmod{n}}$ yields m without ever factoring n.