CS 70 Discrete Mathematics and Probability Theory
Spring 2015 Vazirani HW 6

Reminder: Deadline for HW5 self-grade is Thursday, February 26 at noon.

Reading: Note 7, beginning of Note 8.

Due Monday March 2

1. **RSA lite**

   Woody misunderstood how to use RSA. So he selected prime $P = 101$ and encryption exponent $e = 67$, and encrypted his message m to get $35 = m^e \bmod P$. Unfortunately he forgot his original message m and only stored the encrypted value 35. But Carla thinks she can figure out how to recover m from $35 = m^e \bmod P$, with knowledge only of P and e. Is she right? Can you help her figure out the message m? Show all your work.

   Answer: Recall that the security of RSA depended upon the supposed hardness of factoring $N = P \cdot Q$. However, since $N = P$ in this problem, we can consider it to have been already factored! Indeed, recall that the private key d in RSA is defined to be the multiplicative inverse of e modulo $(P-1)(Q-1)$, because we can then use the following relation to decrypt the message:

   $$m^{k(P-1)(Q-1)+1} \equiv m \pmod{N}$$

   Note that in our case where $N = P$, an analogous relation immediately holds by Fermat's Little Theorem:

   $$m^{k(P-1)+1} \equiv m \pmod{P}$$

   Therefore, if we can find d which is the multiplicative inverse of e modulo $P-1$, we can decrypt the message by simply computing $m^{e \cdot d} \bmod P = 35^d \bmod P$. It is easy to see by inspection that $67 \cdot 3 = 201 \equiv 1 \pmod{100}$, so the desired multiplicative inverse $d = 3$, which means that $m = 35^3 \bmod 101 = 51 \bmod 101$.

   (Otherwise, one can find the multiplicative inverse by applying Extended Euclid's algorithm to $e = 67$ and $P - 1 = 100$:

   $(c, a, b) = \texttt{extended-gcd}(100, 67) = (c, b_1, a_1 - \lfloor 100/67 \rfloor b_1)$ *where*
   $(c, a_1, b_1) = \texttt{extended-gcd}(67, 33) = (c, b_2, a_2 - \lfloor 67/33 \rfloor b_2)$ *where*
   $(c, a_2, b_2) = \texttt{extended-gcd}(33, 1) = (c, b_3, a_3 - \lfloor 33/1 \rfloor b_3)$ *where*
   $(c, a_3, b_3) = \texttt{extended-gcd}(1, 0) = (1, 1, 0)$

   Therefore, $(c, a_2, b_2) = (1, 0, 1)$, $(c, a_1, b_1) = (1, 1, -2)$, *and* $(c, a, b) = (1, -2, 3)$ *respectively. As claimed in Theorem 6.4, we can verify that*

   $$1 = c = ax + by = -2 \cdot 100 + 3 \cdot 67.$$

   Hence, the multiplicative inverse of 67 *modulo* 100 *is* 3.*)*

2. **Fermat and CRT**

In this question we use the Chinese remainder theorem to prove that if $N = PQ$ product of two odd primes, and $\gcd(x,N) = 1$, then $x^{(P-1)(Q-1)} \equiv 1 \pmod{N}$.

(a) First argue that if we know $x^{(P-1)(Q-1)} \equiv y \pmod{P}$ and $x^{(P-1)(Q-1)} \equiv y \pmod{Q}$ then by CRT we can uniquely determine $x^{(P-1)(Q-1)} \equiv y \pmod{N}$.

(b) Compute $x^{(P-1)(Q-1)} \pmod{P}$ and $x^{(P-1)(Q-1)} \pmod{Q}$.

(c) Argue that the unique $y \pmod{N}$ guaranteed by the Chinese remainder theorem must be $y \equiv 1 \pmod{N}$.

Answer:

(a) The Chinese remainder theorem states that there exists a unique $c \pmod{P \cdot Q}$ such that $c \equiv a \pmod{P}$ and $c \equiv b \pmod{Q}$. Setting $a = b = x^{(P-1)(Q-1)}$, we see that y must be the unique c promised by the theorem that satisfies the two given congruences.

(b) We know by Fermat's Little Theorem that $x^{P-1} \equiv 1 \pmod{P}$ and $x^{Q-1} \equiv 1 \pmod{Q}$. (Note that $x \neq 0$ because $\gcd(x,N) = 1$.) Therefore, $x^{(P-1)(Q-1)} \equiv 1^{Q-1} \equiv 1 \pmod{P}$ and $x^{(P-1)(Q-1)} \equiv 1^{P-1} \equiv 1 \pmod{Q}$.

(c) It follows directly from (a) and (b).

3. **Super-RSA?**

Charlie decides that it might be even safer use three prime numbers in place of two from traditional RSA. Suppose he uses primes $P_1 = 3, P_2 = 5, P_3 = 11$ to get $N = P_1P_2P_3 = 165$ and selects $e = 3$.

(a) What is the encryption of the message $m = 10$?

(b) What property should the decryption exponent d satisfy? i.e. how would you calculate d given P_1, P_2, P_3, e? Calculate the decryption exponent for the public key $(N,e) = (165,3)$.

(c) Prove that the decryption function $D(y) = y^d \bmod N$ is the inverse of the encryption function $E(x) = x^e \bmod N$, for your definition of d.

Answer:

(a) $m^e \bmod N = 10^3 \bmod 165 = 10 \bmod 165$. The encryption is 10.

(b) The decryption exponent d must satisfy $de = 1 \bmod (P_1-1)(P_2-1)(P_3-1)$. It is easy to see by inspection that $3 \cdot 27 = 81 \equiv 1 \pmod{80}$, and hence $d = 27$.

(Otherwise, one can find the multiplicative inverse by applying Extended Euclid's algorithm to $e = 3$ and $(P_1-1)(P_2-1)(P_3-1) = 80$:

$(c,a,b) = \texttt{extended-gcd}(80,3) = (c, b_1, a_1 - \lfloor 80/3 \rfloor b_1)$ *where*
$(c,a_1,b_1) = \texttt{extended-gcd}(3,2) = (c, b_2, a_2 - \lfloor 3/2 \rfloor b_2)$ *where*
$(c,a_2,b_2) = \texttt{extended-gcd}(2,1) = (c, b_3, a_3 - \lfloor 2/1 \rfloor b_3)$ *where*
$(c,a_3,b_3) = \texttt{extended-gcd}(1,0) = (1,1,0)$

Therefore, $(c,a_2,b_2) = (1,0,1)$, $(c,a_1,b_1) = (1,1,-1)$, and $(c,a,b) = (1,-1,27)$ respectively. As claimed in Theorem 6.4, we can verify that

$$1 = c = ax + by = -1 \cdot 80 + 27 \cdot 3.$$

Hence, the multiplicative inverse of 3 modulo 80 is $d = 27$.)

(c) We directly follow the proof of Theorem 7.2. It suffices to show that $D(E(x)) = x^{ed} = x \bmod N$, which is equivalent to showing $x^{ed} - x = 0 \bmod N$. Moreover, by definition of d, we know that $ed = 1 \bmod (P_1-1)(P_2-1)(P_3-1)$, i.e., we can write $ed = 1 + k(P_1-1)(P_2-1)(P_3-1)$ for some integer k. Therefore,

$$x^{ed} - x = x^{1+k(P_1-1)(P_2-1)(P_3-1)} - x = x(x^{k(P_1-1)(P_2-1)(P_3-1)} - 1).$$

Our goal is to show that this expression is 0 modulo $N = P_1P_2P_3$ for every x. Since P_1, P_2, P_3 are primes, it is sufficient to show that this expression is divisible by each of P_1, P_2, and P_3.

First, we prove that $x(x^{k(P_1-1)(P_2-1)(P_3-1)} - 1)$ is divisible by P_1. We have two cases to consider:

Case 1: (x *is a multiple of* P_1) In this case, P_1 clearly divides the given expression.

Case 2: (x *is not a multiple of* P_1) Since $x \neq 0 \bmod P_1$, we can use Fermat's Little Theorem to deduce that $x^{P_1-1} = 1 \bmod P_1$. Then $(x^{P_1-1})^{k(P_2-1)(P_3-1)} \equiv 1^{k(P_2-1)(P_3-1)} \bmod P_1$, which implies that $x^{k(P_1-1)(P_2-1)(P_3-1)} - 1 = 0 \bmod P_1$, and so P_1 divides the given expression.

We can use the identical argument to prove that the given expression is also divisible by P_2 and P_3. Therefore, $x^{ed} - x = 0 \bmod N$, as desired.

4. **Digital Signatures**

The RSA crypto system can be used to implement a digital signature scheme. It allows Bob to sign a document m and give Alice $S(m)$ which satisfies the following properties:

(i) If Bob gives the signed document $S(m)$ to Alice, she can verify that Bob signed the document.

(ii) Alice can show $S(m)$ to Carol and convince her that this a copy of document m signed by Bob.

(iii) No one other than Bob can forge his signature on a document.

In this problem:

(a) Show that using Bob's RSA decryption function on m to create $S(m)$ satisfies the first two properties.

(b) Using Bob's RSA decryption function also comes close to satisfying the third property, but not quite. For example, Alice can pick an arbitrary input x, encrypt it using Bob's key and call the result $E(x) = m$. Now if Bob is using his RSA decryption function as the signature, then Alice knows that $S(m) = x$, so Alice can pretend to be Bob sending the document m.

Give a small modification to make the scheme secure against this type of attack. Give an informal justification that your scheme is secure.

Answer:

(a) Let E and D denote Bob's encryption and decryption function respectively. Since D and E are inverses of each other, $E(D(m)) = D(E(m)) = m$. Therefore, if Alice receives the signed document $S(m)$, she can verify that Bob signed the document by simply applying the encryption function E to it and checking that m comes back out. Note that this verification can be carried out by anyone who has Bob's public key and the original document m. Therefore the first two properties are immediately satisfied.

(b) For instance, one can propose that Bob first concatenates the message m with a string of 0's of the same length as m, and then applies his RSA decryption function to the resulting string to produce his signed document. Whoever has Bob's public key and the original document m can

verify the authenticity of the signature by checking that Bob's RSA encryption function returns m concatenated with the right number of 0's.

Since Alice does not have any control over the format of $E(x)$ in the proposed attack, the scheme is secure against this attack.

5. **Bijections**

Let n be an odd number. Let $f(x)$ be a function from $\{0,1,\ldots,n-1\}$ to $\{0,1,\ldots,n-1\}$. In each of these cases say whether or not $f(x)$ is a bijection. Justify your answer (either prove $f(x)$ is a bijection or give a counterexample).

(a) $f(x) = 2x \pmod{n}$.

(b) $f(x) = 5x \pmod{n}$.

(c) n is prime and

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ x^{-1} \pmod{n} & \text{if } x \neq 0 \end{cases}$$

(d) n is prime and $f(x) = x^2 \pmod{n}$.

Answer:

(a) Bijection, because there exists the inverse function $g(y) = 2^{-1}y \pmod{n}$. Since n is odd, we know by Theorem 6.2 that the multiplicative inverse of 2 always exists.

(b) Not a bijection. For example, if $n = 5$, $f(0) = f(1) = 0$.

(c) Bijection, because there exists the inverse function $g(y) = f(y)$. This is an inverse function because the multiplicative inverse is unique (Theorem 6.2).

(d) Not a bijection. For example, if $n = 3$, $f(1) = f(2) = 1$.

6. **Interpolation practice**

Find a polynomial $h(x) = ax^2 + bx + c$ of degree at most 2 such that $h(0) \equiv 2 \pmod{7}$, $h(1) \equiv 4 \pmod{7}$, and $h(2) \equiv 5 \pmod{7}$.

Hint: To do so, first construct three "Delta functions", each a polynomial of degree at most 2, such that

(i) $\Delta_0(0) \equiv 1 \pmod{7}$ and $\Delta_0(x) \equiv 0 \pmod{7}$ for $x = 1, 2$.

(ii) $\Delta_1(1) \equiv 1 \pmod{7}$ and $\Delta_1(x) \equiv 0 \pmod{7}$ for $x = 0, 2$.

(iii) $\Delta_2(2) \equiv 1 \pmod{7}$ and $\Delta_2(x) \equiv 0 \pmod{7}$ for $x = 0, 1$.

Answer: We begin by constructing the three Delta functions suggested in the hint. Using that $\Delta_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}$,

$$\Delta_0(x) = \frac{(x-1)(x-2)}{(0-1)(0-2)} = \frac{1}{2}x^2 - \frac{3}{2}x + 1,$$

$$\Delta_1(x) = \frac{(x-0)(x-2)}{(1-0)(1-2)} = -x^2 + 2x,$$

$$\Delta_2(x) = \frac{(x-0)(x-1)}{(2-0)(2-1)} = \frac{1}{2}x^2 - \frac{1}{2}x.$$

Therefore, the desired polynomial is

$$h(x) = 2\Delta_0(x) + 4\Delta_1(x) + 5\Delta_2(x) = x^2 - 3x + 2 - 4x^2 + 8x + \frac{5}{2}x^2 - \frac{5}{2}x = -\frac{1}{2}x^2 + \frac{5}{2}x + 2.$$

Since the multiplicative inverse of 2 modulo 7 is 4, we can also write

$$h(x) = -4x^2 + 20x + 2 = -4x^2 + 6x + 2 \pmod 7$$

7. **Extra credit**

The Euler totient function $\phi(n)$ is defined to be the number of positive integers less than n (including 1) that are relatively prime to n. Euler's theorem states that $x^{\phi(n)} = 1 \bmod n$ for every x such that $\gcd(x,n) = 1$. You can read more about the Euler totient function at `http://en.wikipedia.org/wiki/Euler's_totient_function`.

For any n, show that the sequence

$$2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \ldots$$

is eventually constant mod n.

Hint: use induction on n and the fact that $\phi(n)$ is strictly less than n.

Answer: We induct on n. The base case $n = 1$ is trivial.

For the induction step, we prove that if the statement is true for all n' smaller than n, then it must be true also for n.

First, observe that if $\gcd(2,n) = 1$, by Euler's theorem, $2^{\phi(n)} = 1 \bmod n$. This implies that $2^x \equiv 2^{x \bmod \phi(n)} \bmod n$, which means that the sequence we are considering is equivalent to

$$2, 2^{2 \bmod \phi(n)}, 2^{(2^2) \bmod \phi(n)}, 2^{(2^{2^2}) \bmod \phi(n)}, \ldots$$

modulo n. However, since $\phi(n) < n$, by induction hypothesis $2 \bmod \phi(n), 2^2 \bmod \phi(n), 2^{2^2} \bmod \phi(n), \ldots$ is eventually constant. Therefore the above sequence must also be eventually constant.

If $\gcd(2,n) \neq 1$, write $n = 2^k m$ where $\gcd(2,m) = 1$. Since $m < n$, by induction hypothesis $2, 2^2, 2^{2^2}, \ldots$ is eventually constant modulo m. Call this constant c. Moreover, observe that $2, 2^2, 2^{2^2}, \ldots$ is eventually constantly 0 modulo 2^k. Then, by Chinese remainder theorem there exists unique $x \pmod n$ such that $x \equiv 0 \pmod{2^k}$ and $x \equiv c \pmod m$. This means that $2, 2^2, 2^{2^2}, \ldots$ will be eventually constantly x modulo n.

It follows by induction that for any n, the sequence $2, 2^2, 2^{2^2}, \ldots$ is eventually constant mod n.

8. **RSA virtual lab**

Follow the virtual lab for this homework (provided on the course website).

(a) Complete all parts and take a screenshot of the page and include it in your homework submission.

(b) Do you think that commitment schemes are necessary for both parties? Is there a protocol simpler than the one introduced in the virtual lab in which only one player encrypts his/her choice using RSA?

Answer: Carefully observing the scheme outlined in the virtual lab, we note that it is necessary only for the first player to encrypt his/her choice. The protocol would look as follows:

Alice Here is my public key: BLAHBLAHBLAHBLAHBLAHBLAH
Alice Here is my encrypted choice: XXXXXXXXXXXXX
Bob Here is my choice: Y
Alice My actual choice was X.

Indeed, Alice cannot cheat because by the time she sees Bob's choice, she has already commited to her choice by revealing the encrypted string. Bob cannot cheat because he cannot tell what Alice's choice is from the encrypted string.