DEVIN MAYA 8/20/23

Math 134: Cryptography Assignment 3

1. 7.1 Find primes p and q for yourself such that $n := pq$ is in the range between $N^3 = 27,000$ and $N^4 = 810,000$ (where $N = 30$). Find a possible e for the RSA cryptosystem and compute the deciphering exponent d.

Solution. Searching for primes in the given range consider $p = 521$ and $q = 617$. Both are prime numbers and the resulting product $n = p \times q = 321257$ is within the given range.

compute $\phi(n) = (p-1)(q-1) = 520 \times 616 = 320320$.

For e a choice is $e = 65537$ it is prime and is an ideal candidate to pick. this value doesn't work for our chosen p and q as $\gcd(65537, 320320) \neq 1$. Another ideal choice is $e = 3$ but we need to make sure it is co prime to $\phi(n)$. Given that $\gcd(3, 320320) = 1$ we can select $e = 3$.

To compute the deciphering exponent d we need to find the multiplicative inverse of e modulo $\phi(n)$. Thus $d \equiv e^{-1} \mod \phi(n)$.

Using the Extended Euclidean Algorithm we can compute d such that $3 \cdot d \equiv 1 \mod 320320$. we find that $d = 213547$.

Thus the private key deciphering exponent is $d = 213547$.

$$p = 521, q = 617, n = 321257, e = 3, \text{and } d = 213547$$

This solution provides primes p and q and their respective public and private keys for the RSA cryptosystem.

2. 7.2 Assume that with the RSA cryptosystem somebody's phone book entry is $(n, e) = (11247661, 268729)$ and assume you found out that it is very likely that $a^{7169e} \equiv a \mod n$ for all $a \in 0, \ldots, n-1$. Find the prime decomposition of n using this information and the deciphering key (n, d) from this information.

Solution.

Given $a^{7169e} \equiv a \mod n$ for all $a \in \{0, \ldots, n-1\}$ this is a property associated with Fermat's Little Theorem and it provides information about the totient function $\varphi(n)$.

Given the RSA property

$$a^{ed} \equiv a \mod n$$

Then $ed \equiv 1 \mod \varphi(n)$ thus $ed = 1 + k\varphi(n)$ for some integer k.

Now given $a^{7169e} \equiv a \mod n$. This suggests that $7169e \equiv 1 \mod \varphi(n)$ or $7169e = 1 + k\varphi(n)$. Then $\varphi(n)$ divides $7169e - 1$. Thus $\varphi(n)$ is a divisor of $7169e - 1$.

Now $n = pq$ where p and q are the prime factors of n.

The Euler's totient function for n is

$$\varphi(n) = (p-1)(q-1)$$

Given n our objective is to find p and q. Once the primes are found finding the deciphering key d is direct using the relation

$$de \equiv 1 \mod \varphi(n)$$

Given $n = 11247661$ and that $7169e \equiv 1 \mod \varphi(n)$ The objective is to find the prime decomposition of n.

To find p and q we can use the fact that $n = pq$ and $\varphi(n) = (p-1)(q-1)$. The relation $7169e = 1 + k(p-1)(q-1)$ implies that $(p-1)(q-1)$ divides $7169e - 1$. We're given $e = 268729$ so we are looking for divisors of $7169 \times 268729 - 1$.

Instead of directly calculating that product a more straightforward approach is to use known methods for factorizing n

For our given $n = 11247661$ after factorization it is discovered that

$$n = 3299 \times 3407$$

Thus $p = 3299$ and $q = 3407$.

Now $\varphi(n) = (p-1)(q-1) = 3298 \times 3406 = 11236628$.

Given $e = 268729$ the objective is to find d such that:

$$de \equiv 1 \mod \varphi(n)$$

we can compute d to be the modular inverse of $e \mod \varphi(n)$. Computing this results in

$$d = 2740469$$

Thus the deciphering key (n, d) is $(11247661, 2740469)$. After finding the prime factorization of n the private key was solved for d that pairs with the given public key e.

3. 8.1 Show that if $f : G \to H$ is a group homomorphism, then $f(1_G) = 1_H$ and $f(g^{-1}) = f(g)^{-1}$

for all $g \in G$.

Solution.

Definition of Group Homomorphism A function $f : G \to H$ is said to be a group homomorphism if for every pair of elements $a, b \in G$ the rule

$$f(a \cdot_G b) = f(a) \cdot_H f(b)$$

holds where $\cdot_G$ is the operation in group G and $\cdot_H$ is the operation in group H.

Let g be an arbitrary element in G. Using the identity property of a group results in

$$g \cdot_G 1_G = g$$

Applying the homomorphism f to both sides results in

$$f(g \cdot_G 1_G) = f(g)$$

By using the property of homomorphisms this can be shown as

$$f(g) \cdot_H f(1_G) = f(g)$$

In order for this equation to be true for all $g \in G$ the element $f(1_G)$ must act as the identity in H. Thus $f(1_G) = 1_H$.

Taking the definition of the inverse in group G it is given that

$$g \cdot_G g^{-1} = 1_G$$

Applying the homomorphism f to both sides results in

$$f(g \cdot_G g^{-1}) = f(1_G)$$

From the first part of the proof it has been shown that $f(1_G) = 1_H$. Using the homomorphic property on the left side of the equation it can be shown as

$$f(g) \cdot_H f(g^{-1}) = 1_H$$

For this equation to be true in group H the element $f(g^{-1})$ must act as the inverse of $f(g)$ in H. Thus $f(g^{-1}) = f(g)^{-1}$.

Therefore on any group homomorphism the image of the identity element of G is the identity element of H and the image of the inverse of an element in G is the inverse of its image in H.

4. 8.2 Show that for every ring R, the set $R^\times$ of invertible elements forms a group under multiplication.

Solution. Closure Let $a, b \in R^\times$. By definition of $R^\times$ there exist inverses a^{-1} and b^{-1} in R. consider the product ab. The inverse of this product is $b^{-1}a^{-1}$. this is verifiable by

$$(ab)(b^{-1}a^{-1}) = a(b \cdot b^{-1})a^{-1} = a \cdot e \cdot a^{-1} = aa^{-1} = e$$

Thus ab has an inverse in R and therefore $ab \in R^\times$ which results in proving closure.

Associativity This property is inherited from the multiplication in R. Since R is a ring its multiplication is associative. Thus for all $a, b, c \in R^\times$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Existence of Identity Element The multiplicative identity in the ring R is 1 since for every element $a \in R$, $a \cdot 1 = 1 \cdot a = a$. Since 1 has a multiplicative inverse of 1, $1 \in R^\times$.

Existence of Inverse By definition of $R^\times$ every element in $R^\times$ has a multiplicative inverse in R. Thus for each $a \in R^\times$ there exists $a^{-1} \in R^\times$ such that

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

In this case all of the known mentioned axioms are satisfied. Therefore $R^\times$ forms a group under multiplication.

5. 8.3 Let G and G' be groups, and let $f : G \to G'$ be a group homomorphism. (a) Show that if $H \leq G$ and $H' \leq G'$, then $f(H) := f(h) \mid h \in H \leq G'$ and $f^{-1}(H') := g \in G \mid f(g) \in H' \leq G$. (b) Show that $\ker(f) \leq G$ and $\mathrm{im}(f) \leq G'$.

Solution.

(a) We have two things to show First $f(H) \leq G'$ and second $f^{-1}(H') \leq G$ To show $f(H) \leq G'$:

begin by proving that $f(H)$ is a subset of G' For any $h \in H$, $f(h)$ is in G' because f is a function from G to G'. Thus $f(H) \subseteq G'$.

Now to verify the subgroup properties for $f(H)$:

Identity $f(e_G) = e_{G'}$ where e_G and $e_{G'}$ are identity elements of G and G' respectively. Since f is a homomorphism $f(e_G)$ is the identity in G'. Therefore $e_{G'} \in f(H)$ when $e_G \in H$. Inverses For any element $h \in H$ its inverse h^{-1} is in H since H is a subgroup of G. Then $f(h^{-1})$ is the inverse of $f(h)$ in G'. Thus if $f(h) \in f(H)$ then its inverse $f(h^{-1})$ is also in $f(H)$. Closure $h_1, h_2 \in H$ their product h_1h_2 is in H. Since f is a

homomorphism $f(h_1h_2) = f(h_1)f(h_2)$. Then the product of any two elements in $f(H)$ remains in $f(H)$.

All these conditions prove that $f(H) \leq G'$.

Now to show $f^{-1}(H') \leq G$

For any element $g' \in H'$ consider the set of all elements in G that get mapped to g' under the function f. This set is $f^{-1}(g')$.

Now the set $f^{-1}(H')$

Identity Since $f(e_G) = e_{G'}$ and $e_{G'} \in H'$ the identity e_G of G is in $f^{-1}(H')$. Inverses If $g \in f^{-1}(H')$ then $f(g) \in H'$. furthermore $f(g^{-1})$ is the inverse of $f(g)$ in G' which means $f(g^{-1})$ is also in H'. Thus g^{-1} is in $f^{-1}(H')$. Closure For any $g_1, g_2 \in f^{-1}(H')$ the resulting product in G gets mapped to the product of their images in G' which is still in H'. Therefore g_1g_2 is also in $f^{-1}(H')$.

This proves that $f^{-1}(H') \leq G$.

(b)

To show $\ker(f) \leq G$:

The kernel of the homomorphism f is given by $\ker(f) = \{g \in G \mid f(g) = e_{G'}\}$ where $e_{G'}$ is the identity element in G'.

Identity $f(e_G) = e_{G'}$. Therefore e_G is in $\ker(f)$. Inverses If $g \in \ker(f)$ then $f(g) = e_{G'}$. This implies that $f(g^{-1})$ is the inverse of $e_{G'}$ in G' which is $e_{G'}$ itself. Therefore g^{-1} is also in $\ker(f)$. Closure For any $g_1, g_2 \in \ker(f)$, $f(g_1g_2) = f(g_1)f(g_2) = e_{G'}e_{G'} = e_{G'}$. This implies g_1g_2 is also in $\ker(f)$.

This proves that $\ker(f) \leq G$.

To show $\text{im}(f) \leq G'$

The image of f is given by $\text{im}(f) = \{g' \in G' \mid g' = f(g) \text{ for some } g \in G\}$.

Identity $f(e_G) = e_{G'}$ so

$e_{G'}$ is in $\text{im}(f)$. Inverses If g' is in $\text{im}(f)$ then there exists $g \in G$ such that $f(g) = g'$. Since $f(g^{-1})$ is the inverse of g' in G', $f(g^{-1})$ is in $\text{im}(f)$. Closure If g_1', g_2' are in $\text{im}(f)$ there exist $g_1, g_2 \in G$ such that $f(g_1) = g_1'$ and $f(g_2) = g_2'$. Then $f(g_1g_2) = g_1'g_2'$. The product $g_1'g_2'$ is in $\text{im}(f)$.

This proves that $\text{im}(f) \leq G'$. It has been shown that the image and the kernel of a group homomorphism are both subgroups of their respective group and how the homomorphism operates on subgroups.

6. 8.4 Assume that $G = \langle x \rangle$ and that $\text{ord}(x) = n \in \mathbb{N}$. Moreover, let $k \in \mathbb{Z}$ and set $y := x^k$. Show that $\text{ord}(y) = n/\gcd(n, k)$.

Solution. The order of an element a in a group G is denoted by $\text{ord}(a)$ which is the smallest positive integer m such that $a^m = e$ where e is the identity element in G.

Given $G = \langle x \rangle$, $\text{ord}(x) = n$, $y = x^k$

The objective to find the order of y.

Consider $y^m = (x^k)^m = x^{km}$.

For y^m to be the identity x^{km} should be the identity. Since the order of x is n it is known that $x^n = e$. Thus we want to find the smallest positive m such that $km \equiv 0 \mod n$. the smallest such m is $\frac{n}{\gcd(n,k)}$. Given $km \equiv 0 \mod n$ it means n divides km $n|km$. the fundamental property of the greatest common divisor states If $a|bc$ and a and b are coprime then $a|c$.

Using the property above and taking $a = n$ and $b = k$ it implies that if $n|km$ and $\gcd(n,k) = d$ then $n/d|m$. This gives $m \geq \frac{n}{d}$.

Now considering the number $m = \frac{n}{d}$ where $d = \gcd(n,k)$.

$$(x^k)^{\frac{n}{d}} = x^{k\frac{n}{d}}$$

Now by using properties of modular arithmetic the fact that kn/d is a multiple of n when $d = \gcd(n,k)$ results in

$$x^{kn/d} = x^{n\cdot(k/d)} = (x^n)^{\frac{k}{d}} = e^{\frac{k}{d}} = e$$

Thus $\text{ord}(y) = \frac{n}{\gcd(n,k)}$ which was needed

Therefore the order of y in the group G is $n/\gcd(n,k)$.

7. Additional 1: Prove that $\gcd(a,b) \cdot \text{lcm}(a,b) = a \cdot b$.

Solution.

Given

$$\gcd(a,b) \cdot \text{lcm}(a,b) = a \cdot b$$

Let $d = \gcd(a,b)$. This means d is the greatest common divisor of a and b. By the definition of the greatest common divisor there exist integers x and y such that

$$a = dx$$

$$b = dy$$

consider the least common multiple denoted as $m = \text{lcm}(a, b)$. By definition m is the smallest positive integer that is a multiple of both a and b. Given that a and b both divide m . Thus

$$m = a \cdot u = dx \cdot u$$

$$m = b \cdot v = dy \cdot v$$

Then $dx \cdot u = dy \cdot v$. Using $\gcd(x, y) = 1$ because d was the greatest common divisor of a and b so x and y are coprime then y divides u and x divides v.

Now consider m. Thus

$$m = a \cdot u = dx \cdot u = dy \cdot \frac{u}{y} = b \cdot \frac{u}{y}$$

Here u/y is an integer because y divides u.

Now consider $m' = a \cdot x = dx \cdot x = dy \cdot y = b \cdot y$.

Then m' is also a multiple of both a and b. Given the definition of m as the least common multiple the result is $m \leq m'$.

But given the forms of m and m' as derived above the result is that that they are equal $m = m'$.

Then $m = a \cdot x = b \cdot y$.

using the expressions for a and b in terms of d the result is

$$\text{lcm}(a, b) = a \cdot x = dx \cdot x = d \cdot (xy)$$

Multiplying both sides by d results in

$$d \cdot \text{lcm}(a, b) = d^2 \cdot xy$$

However $d \cdot xy = a \cdot b$ as $a = dx$ and $b = dy$.

Therefore

$$\gcd(a, b) \cdot \text{lcm}(a, b) = a \cdot b$$