Jason Dykstra

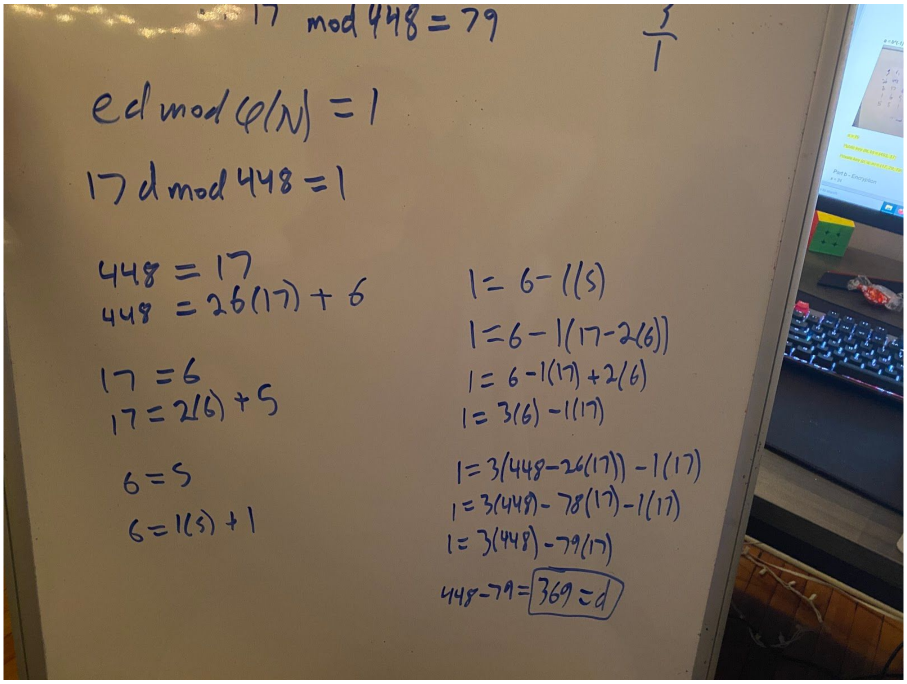
Problem 1 - Computing RSA By Hand

p = 17
q = 29
b = 17

Part a - Key Generation

N = p*q
N = 17*29 = 493

φ(N) = (p - 1)*(q - 1)
φ(N) = 16*28 = 448



$17 \bmod 448 = 79$

$\frac{3}{1}$

$ed \bmod \varphi(N) = 1$

$17d \bmod 448 = 1$

$448 = 17$
$448 = 26(17) + 6$

$17 = 6$
$17 = 2(6) + 5$

$6 = 5$
$6 = 1(5) + 1$

$1 = 6 - 1(5)$
$1 = 6 - 1(17 - 2(6))$
$1 = 6 - 1(17) + 2(6)$
$1 = 3(6) - 1(17)$

$1 = 3(448 - 26(17)) - 1(17)$
$1 = 3(448) - 78(17) - 1(17)$
$1 = 3(448) - 79(17)$
$448 - 79 = \boxed{369 = d}$

a = d (from image) = 369

Public key (N; b) = (493, 17)

Private key (p; q; a) = (17, 29, 369)

Part b - Encryption

x = 31

$y = x^b \bmod N$
$y = 31^{17} \bmod 493$

Exponent in binary: 17 base 2 = 10001

Bit 1 (1):		31 mod 493	= 31
Bit 2 (0):	31^2	= 961 mod 493	= 468
Bit 3 (0):	468^2	= 219024 mod 493	= 132
Bit 4 (0):	132^2	= 17424 mod 493	= 169
Bit 5 (1):	$169^2 * 31$	= 885391 mod 493	= 456

This means that the encrypted message is 456.

Part c - Decryption

x = y^a mod N
x = 456^369 mod 493

Exponent in bit form: 369 base 2 = 101110001

Bit 1 (1):		456 mod 493	= 456
Bit 2 (0):	456^2	= 207936 mod 493	= 383
Bit 3 (1):	$383^2 * 456$	= 66890184 mod 493	= 437
Bit 4 (1):	$437^2 * 456$	= 87081864 mod 493	= 316
Bit 5 (1):	$316^2 * 456$	= 45534336 mod 493	= 363
Bit 6 (0):	363^2	= 131769 mod 493	= 138
Bit 7 (0):	138^2	= 19044 mod 493	= 310
Bit 8 (0):	310^2	= 96100 mod 493	= 458
Bit 9 (1):	$458^2 * 456$	= 95652384 mod 493	= 31

This means that the plaintext is 31, the same as we encrypted!

Part d - Attack

i. y = x^b mod N, and x = y^a mod N. Eve knows the public key N of 493 and the b value of 17, thus it is possible to recover the plaintext. The totient of N can be found by doing prime factorization of 493 and then computing the private key to decrypt the message.

ii. p and q, the two primes used to create N are not publicly known, however it is possible for Eve to discover them by factoring (especially with p and q being so small in this example). This means it is possible for Eve to recover φ(N), and thus the private key a.

iii. The only factors of 493 are 17 and 29, which means Eve can find φ(N) by simply doing (17-1)*(29-1) = 448.
Then, Eve can use φ(N) to compute a the same way as shown in my answer to part a.
Finally, Eve can simply use the formula x = y^a mod N to decipher the message, which would result in x = 31, the correct answer.

iv. Doing the same task for a large N such as one with 1024 digits would be near impossible since the time it would take to find the prime factors of such a number is not yet efficient enough with our technology. This key space would be an enormous number such as 2^{8192}

v. Given only a message-ciphertext pair, the strength of the public key would determine whether or not Eve could find the private key. If the public key is as weak as the one in the example (493, 17) then Eve could find the factors of N very quickly and continue the steps in part iii above to find the private key. If the public key N value was very large, however, Eve would not be able to recover the private key. If Eve did not know the public key at all, then she would be unable to find the private key since multiple RSA setups could encrypt different plaintexts to the same ciphertext, and Eve would have no idea which model was correct.

Problem 2 - Proof Of Correctness Of RSA

Only two cases, where the gcd(x, N) = 1, and where gcd(x, N) ≠ 1
(where x is the plaintext)

First let's look at where gcd(x, N) = 1:

This is normal RSA, meaning Euler's theorem applies, meaning:
$x^{\varphi(N)} = 1 \bmod N$
This is simply a reinstatement of what I did earlier in the homework.

Now, we are trying to prove that: $(x^e)^d = x \bmod N$, for all $x \in \bmod N$, so we can now write:
$(x^e)^d = x^{ed} = x^{1+k\varphi(N)}$
$x^{1+k\varphi(N)} = x{*}x^{k\varphi(N)} = x{*}(x^{\varphi(N)})^k$

Applying Euler’s theorem:
$x{*}(x^{\varphi(N)})^k = x \bmod N$

This proves that all cases under gcd(x, N) = 1 work!

Second case: gcd(x, N) ≠ 1
Because the gcd is not 1, we can not use Euler’s theorem.

However, since we know that gcd(p, q) = 1 we know that:
$x = y \pmod p \land x = y \pmod q \Rightarrow x = y \pmod{pq}$

Additionally, since gcd(x, N) ≠ 1, either gcd(x, N) = p or gcd(x, N) = q must be true.

Let’s look at the first scenario: If gcd(x, N) = p then it is implied that x = kp for some k > 0.
This means that x mod p = 0. From this information we can create this relationship:
$(m^e)^d = ((kp)^e)^d$
Which is a multiple of p, meaning it is equal to 0. We get that 0 = 0 thus proving this first case true.

For the second scenario: gcd(x, N) = q we can apply Eurler’s theorem since we know gcd(x, q) = 1 since q is a prime. Thus:
$x^{\varphi(q)} = 1 \bmod q$

From this, we can simplify:
$(x^e)^d = x^{ed}$
$= x^{ed - 1}x$
$= x^{h(p-1)(q-1)}x$
$= (x^{q-1})^{h(p-1}x$
$= 1^{h(p-1)}x = x \bmod q$

This proves the second statement true, meaning both gcd(x, N) = p and gcd(x, N) = q are true, proving gcd(x, N) ≠ 1 true for all x ∈ mod N!