Carl Cortez

CIS 628

Chapter 7

Lab 8

7.1

Lab 8

task1 primes for RSA

7.1) $P=41$ and $Q=17$; $e_1=32$ or $e_2=49$

$n=41\cdot 17$

$\Phi(41\cdot 17)=40\cdot 16=640$; Now find which $GCD(640,e)=1$

① $640=20\cdot 32+0 \Rightarrow GCD(640,32)=32\neq 1$ No good!

② $640=13\cdot 49+3$

$49=16\cdot 3+1$

$3=3\cdot 1+0 \Rightarrow GCD(640,49)=1$ ✓ $\Rightarrow e_2=49$ is a valid RSA exponent.

task 2 Private Key $K_{pr}=(P,q,d)=(41,17,d)$ $e=49$

$d\cdot e \equiv \bmod 640 \Rightarrow d\cdot 49 \equiv \bmod 640$

$3=640-13\cdot 49$

$1=49-16\cdot 3=49-16(640-13\cdot 49)$ $t=d$

$209(49)-16(640)=-16(640)+209(49)$

So, $K_{pr}=(41,17,209)$

7.2

$$\begin{array}{cccccccc} 0 & \cancel{1} & \cancel{0} & \cancel{0} & \cancel{1} & 1 & 1 & 1 \\ & 64 & 32 & 16 & 8 & 4 & 2 & 1 \end{array}$$

7.2

Final Answer: 42

$x^e \bmod m$ using square + multiply

task 1) $x=2$ $e=79$ mod 101

$2^{79} = 2^{1001111_2}$ $h_6 = 1$ ← start!

h_5 $X = 2^{1_2}$ | $h_5 = 0$ $(2^1)^2 = 2^2 = 2^{10_2}$; no mul! BC $h_5 = 0$

$h_4 = 0$ $(2^2)^2 = 2^4 = 2^{100_2}$; no mult, BC $h_4 = 0$ | 16

$h_3 = 1$ $(2^4)^2 = 2^8 = 2^{1000_2}$; MULT! $h_3 = 1$

$2^8 \cdot 2 = 2^9 = 2^{1001_2}$ 512 mod 101 = 7

$h_2 = 1$ $(2^9)^2 = 2^{18} = 2^{10010_2}$; MULT! $h_2 = 1$

$(2^{18}) \cdot 2 = 2^{19} = 2^{10011_2}$ $\}$ 98

$h_1 = 1$ $(2^{19})^2 = 2^{38} = 2^{100110_2}$; MULT!

$(2^{38}) \cdot 2 = 2^{39} = 2^{100111_2}$ $\}$ 18

$h_0 = 1$ $(2^{39})^2 = 2^{78} = 2^{1001110_2}$ MULT!

$(2^{78}) \cdot 2 = 2^{79} = 2^{1001111_2}$ $\}$ $\boxed{42}$

$$\left(\left(\left(\left(\left(x^2\right)^2\right)^2 \cdot x\right)^2 \cdot x\right)^2 \cdot x\right)^2 \cdot x$$

$7^2 \cdot 2 \equiv 98 \bmod 101$

$98^2 \cdot 2 \equiv 18 \bmod 101$

$18^2 \cdot 2 \equiv 42 \bmod 101$

task 2 $\cancel{\underset{128}{1}}\ \cancel{\underset{64}{1}}\ \cancel{\underset{32}{0}}\ \cancel{\underset{16}{0}}\ \cancel{\underset{8}{0}}\ \underset{4}{1}\ \underset{2}{0}\ \underset{1}{1}$

$x=3 \quad e=197 \quad m=101$

Final Answer
15

$3^{197} = 3^{11000101_2}$ $\quad h_7=1$

★ initial setting $X = X^{1_2}$

9
27

$h_6=1$ $\quad (X)^2 = X^2 = X^{10_2}$ Multiply! S+M
$X^2 \cdot X = X^3 = X^{11_2}$

$h_5=0$ $\quad (X^3)^2 = X^6 = X^{110_2}$ No Multiply S $\quad 729 \equiv 22 \bmod 101$

$h_4=0$ $\quad (X^6)^2 = X^{12} = X^{1100_2}$ No Multiply S $\quad$ ~~[illegible]~~ 531,441
80

$h_3=0$ $\quad (X^{12})^2 = X^{24} = X^{11000_2}$ No Multiply S $\quad$ 282,429,536,481
37

$\cancel{h_2}=1$ $\quad (X^{24})^2 = X^{48} = X^{110000_2}$ Multiply! ~~S+M~~ $\}$ 67
$(X^{48}) \cdot X = X^{49} = X^{110001_2}$

$h_1=0$ $\quad (X^{49})^2 = X^{98} = X^{1100010_2}$ No Multiply ~~S~~ $\}$ 45

$h_0=1$ $\quad (X^{98})^2 = X^{196} = X^{1100\,0100}$ Multiply ~~S+M~~ $\}$ 15
$(X^{196}) \cdot X = X^{197} = X^{1100\,0101}$ ✓

$$\left(\left(\left(\left(\left(\left(3^2\cdot 3\right)^2\right)^2\right)^2\right)^2\cdot 3\right)^2\right)^2\cdot 3$$

$22^2 \equiv 80 \bmod 101$
$80^2 \equiv 37 \bmod 101$
$37^2 \cdot 3 \equiv 67 \bmod 101$
$67^2 \equiv 45 \bmod 101$
$45^2 \cdot 3 \equiv 15 \bmod 101$

7.3

7.3

Encrypt + decrypt by means of RSA

1) $p=3, q=11, d=7, x=5$

Encrypt: $y = e_{k_{pub}}(x) \equiv x^e \bmod n$ Decrypt: $x = d_{k_{pr}}(y) \equiv y^d \bmod n$

- $n = 3 \cdot 11 = 33$
- $\Phi(33) = 2 \cdot 10 = 20$
- $\boxed{e=3}$ since $d \cdot e \equiv_{\bmod 20} 1$

So, $K_{pub} = (33,3)$, $Y = X^e \equiv 5^3 = 3 \cdot 33 + 26$

$Y = X^e \equiv_{\bmod 33} 26$

task 2

$p=5 \quad q=11 \quad e=3 \quad x=9$

$n=55 \Rightarrow \Phi(55) = (4)(10) = 40$

$d \cdot e \equiv_{\bmod 40} 1$ $\quad$ $81 \bmod 40 = 1$

$3 \cdot d \equiv_{\bmod 40} 1$ $\quad$ $3 \cdot 27$ ✓

$d = 27$

$Y \equiv 9^3 \bmod 55 = 14 = Y$

$729 = 13 \cdot 55 + 14$

7.5

In practice the short exponents e = 3, 17 and 216 +1 are widely used. 1. Why can't we use these three short exponents as values for the exponent d in applications where we want to accelerate decryption?

Since these are, "widely used," I would assume that people are aware of these short exponents.

This reminds me of the time I hacked free wi-fi during college. I took some password guesses on a neighboring wi-fi network and had success with ***password*** as the password. A simple guess on ideal passwords/solutions could be used in this dynamic. It's not wise to use common passwords or in this case short exponents because they can be easily guessed and brute forced.

2. Suggest a minimum bit length for the exponent d and explain your answer.

From page 184 of the textbook, they mention 128 bits being a larger number to avoid brute-force. I imagine this is a good start for bit lengths of exponent d. If we were to exceed 128 bits, I imagine that would improve the security even more.

7.11

In this exercise, you are asked to attack an RSA encrypted message. Imagine being the attacker: You obtain the ciphertext y = 1141 by eavesdropping on a certain connection. The public key is kpub = (n,e)=(2623,2111).

1. Consider the encryption formula. All variables except the plaintext x are known. Why can't you simply solve the equation for x?

Initially, I thought an answer could be retrieved using properties of logs. However, these outcomes for x^e can be congruent to a variety of outcomes.

2. In order to determine the private key d, you have to calculate d ≡ e−1 mod Φ(n). There is an efficient expression for calculating Φ(n). Can we use this formula here?

We're lucky enough to know what ***n*** and ***e*** are. However, from the equation of Φ(n), we need to know the two prime numbers used in the product (p and q). Since we don't have those, we cannot use the formula here.

3. Calculate the plaintext x by computing the private key d through factoring $n = p \cdot q$. Does this approach remain suitable for numbers with a length of 1024 bit or more?

7.11

Task 3

$Y = 1141$

$K_{pub} = (n, e) = (2623, 2111)$

Goal

Find Plaintext by computing private key d through factoring $n = p \cdot q$.
Does it work for numbers ≥ 1024 bits.

Work shown in previous labs to why this works.

- $2623 = 43 \cdot 61 = p \cdot q$
- $\Phi(n) = \Phi(2623) = \Phi(43 \cdot 61) = (42)(60) = 2520$

$e \cdot d \equiv \bmod \Phi n$

cc: Page 194

$d^{-1} \equiv e \bmod \Phi(n)$ $\Rightarrow d \equiv e^{-1} \bmod \Phi(n)$

$X \equiv Y^d \bmod n$

$2520 = 2111 + 409$
$2111 = 409 \cdot 5 + 66$
$409 = 6(66) + 13$
$66 = 5(13) + 1$
$13 = 13(1) + 0$

$409 = 2520 - 2111$
$66 = 2111 - 5(409)$
$= 2111 - 5(2520 - 2111)$
$6(2111) - 5(2520)$
$13 = 409 - 6(66)$
$409 - 6[6(2111) - 5(2520)]$
$[2520 - 2111]$
$30(2520) - 37(2111)$
$1 = 66 - 5(13)$
$[6(2111) - 5(2520)] - 5[30(2520) - 37(2111)]$

$191(2111) - 155(2520) = 1$
$-155(2520) + 191(2111) = 1$
$e^{-1} = 191$

SO!

$d \equiv e^{-1} \bmod (2520) = \boxed{191}$

★Find X!

$X \equiv 1141^{191} \bmod 2623$

Next page!

$\cancel{\frac{1}{128}}\ \cancel{\frac{0}{64}}\ \cancel{\frac{1}{32}}\ \cancel{\frac{1}{16}}\ \cancel{\frac{1}{8}}\ \frac{1}{4}\ \frac{1}{2}\ \frac{1}{1}$

h_7 h_0

$X = 1141^{191} \bmod 2623$

Final Answer

$X = 1088$

Start

$h_7 = 1$ $1141^{1011\,1111_2}$

1141^1

$h_6 = 0$

$(1141^1)^2 \Rightarrow 1141^2$ No multiply ~~S~~ 873

$h_5 = 1$

$(1141^2)^2 \Rightarrow 1141^4 = 1141^{100_2}$ multiply! ~~S+M~~

$(1141^4) \cdot 1141 = 1141^5 = 1141^{101_2}$ 1737

$h_4 = 1$

$(1141)^{10}$ multiply ~~S+M~~

$(1141)^{11}$ 1552

$h_3 = 1$

$(1141)^{22}$ multiply $(1141)^{23}$ ~~S+M~~

$h_2 = 1$

$(1141)^{46}$ multiply $(1141)^{47}$ ~~S+M~~

$h_1 = 1$

$(1141)^{94}$ $(1141)^{95}$ ~~S+M~~

$h_0 = 1$

$(1141)^{190} \Rightarrow (1141)^{191}$ ~~S+M~~

$$\left(\left(\left(\left(\left(\left((X)^2\right)^2 \cdot X\right)^2 \cdot X\right)^2 \cdot X\right)^2 \cdot X\right)^2 \cdot X\right)^2 \cdot X$$

$1141^2 \equiv 873 \bmod 2623$

$873^2 \cdot 1141 \equiv 1737 \bmod 2623$

$1737^2 \cdot 1141 \equiv 2003 \bmod 2623$

$2003^2 \cdot 1141 \equiv 701 \bmod 2623$

$701^2 \cdot 1141 \equiv 1307 \bmod 2623$

$1307^2 \cdot 1141 \equiv 154 \bmod 2623$

$154^2 \cdot 1141 \equiv 1088 \bmod 2623$