1 Primes and Factoring

Recall a prime is an integer greater than 1 whose only positive integer divisors are itself and 1. Suppose you have a process that is done and undone by multiplying primes (i.e., done by multiplying primes or powers of primes and undone by factoring a number into its prime divisors (prime factorization)). Are these processes equally easy?

Example:

(a) Multiply 23*47 = 1081

(b) Multiply 31*52. = $31 \cdot 2^2 \cdot 13 = 1612$

(c) Determine the prime factorization of 1711. $= 29 \cdot 59$

(d) Determine the prime factorization of 918. $= 2 \cdot 3^3 \cdot 17$

$918 \div 2 = 459$ $459 \div 3 = 153$ $153 \div 3 = 51$ $51 \div 3 = 17$

Example: Is there a largest prime? Why or why not?

No - Suppose x_n is the largest prime. Then for primes $x_1, x_2, \ldots x_n$, $x_1 \cdot x_2 \cdot \ldots \cdot x_n = y$. But we know $(y+1)$ is not divisible by $x_1, x_2, \ldots x_n$ so $y+1$ is prime - contradiction of assumption

2 Encoding with the RSA Method

Definitions:

The (relative) ease of multiplying primes and difficulty of factoring numbers into primes is the foundation of the RSA method (developed by Rivest, Shamir, & Adleman in the 1970s). This method is a type of public-key cryptography, where anyone can encipher but only someone with a particular key can decipher. To encipher, we first translate our text to numbers called plaintext (e.g., 00 for space, 01-26 for A through Z), then use modular exponentiation where we raise to a power E (for encipher) in $\mathbb{Z}_n$. That is for plaintext $P_1, P_2, P_3\ldots$ the ciphertext is $C_1, C_2, C_3\ldots$ where for each i, $C_i \equiv P_i^E \pmod{n}$, $0 \le C_i < n$. The n that is chosen needs to be a product of 2 distinct primes.

Example: Suppose $n = 33$, $E = 7$ and we want to encipher "HELLO WORLD".

(a) Convert "HELLO WORLD" to plaintext using 00 for space, and 01-26 for A through Z.

00 space	08 H	16 P	24 X
01 A	09 I	17 Q	25 Y
02 B	10 J	18 R	26 Z
03 C	11 K	19 S	27 ?
04 D	12 L	20 T	28 .
05 E	13 M	21 U	29 ,
06 F	14 N	22 V	30 :
07 G	15 O	23 W	31 ;
			32 '

H E L L O (space)
08 05 12 12 15 00

W O R L D
23 15 18 12 04

plaintext

(b) Encipher (create ciphertext) using modular exponentiation. $C_i \equiv P_i^E \pmod{n}$

$8^7 \pmod{33}$, $8^7 = 2{,}097{,}152$ 2097152/33 & get remainder of 2

Thus $2 \equiv 8^7 \pmod{33}$ (P of 8 leads to C of $\underline{2}$)

$5^7 \pmod{33}$ – nearest divisible by 33 is 78111, $78125 - 78111 = 14$ $5^7 \equiv \underline{14} \pmod{33}$
$(5^7 = 78125)$

$12^7 = 35{,}831{,}808$ – nearest div by 33 is 35,831,796 $12^7 \equiv 12 \pmod{33}$

$15^7 = 170{,}859{,}375$ – nearest is 170,859,348 $15^7 \equiv 27 \pmod{33}$

$0^7 = 0$

$23^7 = 3{,}404{,}825{,}447$ – nearest is 3,404,825,424 $23^7 \equiv 23 \pmod{33}$

$18^7 = 612220032$ – nearest is 61,222,026 $18^7 \equiv 6 \pmod{33}$

$4^7 = 16{,}384$ – nearest 16,368 $4^7 \equiv 16 \pmod{33}$

ciphertext: 02 14 12 12 27 00 23 27 06 12 16

(c) (Optional) Convert back to letters.

BNLL? _ W?FLP
(space)

Using $n = 33$, we only had space to characterize uppercase letters, a space, and a few other symbols. In general, we may want to distinguish upper and lowercase letters and include numbers and other symbols or keystrokes so larger n's are often necessary to accomodate what we need to be able to say. However, that means our bases (P) and exponents (E) can get much bigger.

Example: Suppose $P = 19$, $E = 41$, $n = 91$. Can we use a calculator to directly translate P to ciphertext C? Why or why not? $19^{41} \bmod 91$

Calculator gives a number E52 ($\ast \times 10^{52}$) – don't know precise number to check against – we need a new technique

Example: Suppose $P = 19$, $E = 41$, $n = 91$. Translate P to ciphertext C.

$19^{41} = 19^{32} \cdot 19^{8} \cdot 19^{1}$ $32+8+1=41$ ~ use largest powers of 2 available at each step

32 largest in 41 ~ now 9 left

8 largest in 9 – 1 left

$19^1 \equiv 19 \bmod 91$

$19^2 \equiv 19 \cdot 19 \equiv 361 \equiv 88 \equiv -3 \pmod{91}$

$19^4 \equiv 19^2 \cdot 19^2 \equiv (-3)(-3) \equiv 9 \pmod{91}$

$19^8 \equiv 19^4 \cdot 19^4 \equiv (9)(9) \equiv 81 \pmod{91} \equiv -10 \pmod{91}$

$19^{16} \equiv 19^8 \cdot 19^8 \equiv (-10)(-10) \equiv 100 \equiv 9 \pmod{91}$

$19^{32} \equiv 19^{16} \cdot 19^{16} \equiv (9)(9) \equiv -10 \pmod{91}$

$19^{41} \equiv 19^{32} \cdot 19^{8} \cdot 19^{1} \equiv (-10)(-10)(19) \equiv 1900 \bmod 91 \equiv 80 \bmod 91$

Ciphertext $C = 80$

Example: Suppose $P = 7, E = 53, n = 123$. Translate P to ciphertext C.

$7^{53} \equiv C \pmod{123}$ $7^{53} = 7^{32} \cdot 7^{16} \cdot 7^{4} \cdot 7^{1}$

$53 - 32 = 21$
-16
5

$7^1 \equiv 7 \bmod 123$

$7^2 \equiv 49 \bmod 123$

$7^4 \equiv (49)(49) \equiv 2401 \equiv 64 \pmod{123}$

$7^8 \equiv (64)(64) \equiv 4096 \equiv 37 \pmod{123}$

$7^{16} \equiv (37)(37) \equiv 1369 \equiv 16 \pmod{123}$

$7^{32} \equiv (16)(16) \equiv 256 \equiv 10 \pmod{123}$

$7^{53} \equiv 7^{32} \cdot 7^{16} \cdot 7^{4} \cdot 7^{1} \equiv (10)(16)(64)(7) \equiv 71680 \equiv \underline{94} \pmod{123}$

$C = 94$

Theorem 3.5:

If the integer $n > 1$ is not prime, then n has a prime factor no larger than $\sqrt{n}$.

Why is this helpful?

when determining prime factors, we can stop when we go down w/ products OR if we haven't hit a factor yet & reach $\sqrt{n}$, we can stop & conclude n is prime

3 Deciphering with RSA

The exponent D used for deciphering is the smallest positive possible solution x to the congruence $Ex \equiv 1 \pmod{b}$, where $b = (p-1)(q-1)$ and $\gcd(E, b) = 1$. To solve, we can use the extended Euclidean Algorithm as in Section 3.2. $(n = pq)$

Example: Using $P = 19$, $E = 41$, $n = 91$:

(a) Find b corresponding to $n = 91$, where b and n are as in the RSA method.

$7 \cdot 13$ (p, q) $\quad b = (7-1)(13-1) = 6(12) = 72$

(b) Use the extended Euclidean algorithm to find the value of D corresponding to the constants above. $41x \equiv 1 \pmod{72} \Rightarrow \underline{41x + 72y = 1} \quad E = 41$

$41 = 0(72) + 41$
$72 = 1(41) + 31 \rightarrow 72 - 1(41) = 31$
$41 = 1(31) + 10 \rightarrow 41 - 1(31) = 10$
$31 = 3(10) + 1 \rightarrow 31 - 3(10) = 1$
$10 = 10(1) + 0$

$31 - 3(41 - 1(31)) = 1$
$\Rightarrow 31 - 3(41) + 3(31) = 1$
$\Rightarrow 4(31) - 3(41) = 1$
$\Rightarrow 4(72 - 1(41)) - 3(41) = 1$
$\Rightarrow 4(72) - 4(41) - 3(41) = 1$
$\Rightarrow 4(72) - 7(41) = 1$
$y = 4 \quad x = -7$
$41(-7) + 72(4) = 1$

$41(-7) \equiv 1 \bmod 72 \qquad -7$ is not between 0 & 71
$-7 + 72 = \boxed{65 = D}$

Why is this method secure?

Finding b is nontrivial for large values n (products of primes)

4 Practicing Everything Together

Suppose $n = 187$, $P = 13$, $E = 73$.

(a) Translate P to ciphertext C.

$13^{73} \equiv C \pmod{187}$

$73 - 64 = 9$

$13^{64} \cdot 13^{8} \cdot 13^{1} = 13^{73}$

$13^1 \equiv 13 \pmod{187}$

$13^2 \equiv 169 \pmod{187} \equiv -18 \bmod 187$

$13^4 \equiv (-18)(-18) \equiv 324 \equiv 137 \equiv -50 \bmod 187$

$13^8 \equiv (-50)(-50) \equiv 2500 \equiv 69 \bmod 187$

$13^{16} \equiv (69)(69) \equiv 4761 \equiv 86 \bmod 187$

$13^{32} \equiv (86)(86) \equiv 7396 \equiv 103 \bmod 187$

$13^{64} \equiv (103)(103) \equiv 10609 \equiv 137 \bmod 187$

$13^{73} \equiv 13^{64} \cdot 13^{8} \cdot 13^{1} \equiv (137)(69)(13) \equiv 122889 \equiv 30 \bmod 187$

$\boxed{C = 30}$

(b) Find b corresponding to n, where b and n are as in the RSA method.

$n = 187 = \underset{p}{11} \cdot \underset{q}{17}$

$b = (p-1)(q-1) = (11-1)(17-1) = (10)(16) = 160$

(c) Use the extended Euclidean algorithm to find the value of D corresponding to the constants above. $\gcd(160, 73) = 1$ ✓ $Ex \equiv 1 \bmod b$ $73x \equiv 1 \bmod 160$

aka $73x + 160y = 1$

$160 = 2(73) + 14 \rightarrow 160 - 2(73) = 14$

$73 = 5(14) + 3 \rightarrow 73 - 5(14) = 3$

$14 = 4(3) + 2 \rightarrow 14 - 4(3) = 2$

$3 = 1(2) + 1 \rightarrow 3 - 1(2) = 1$ gcd

$2 = 2(1) + 0$

$3 - 1(14 - 4(3)) = 1$

$\Rightarrow 3 - 1(14) + 4(3) = 1$

$\Rightarrow 5(3) - 1(14) = 1$

$\Rightarrow 5(73 - 5(14)) - 1(14) = 1$

$\Rightarrow 5(73) - 25(14) - 1(14) = 1$

$\Rightarrow 5(73) - 26(14) = 1$

$\Rightarrow 5(73) - 26(160 - 2(73)) = 1$

$\Rightarrow 5(73) - 26(160) + 52(73) = 1$

$\Rightarrow \underline{57}(73) - 26(160) = 1$

$0 < 57 < 160$ ✓

$\boxed{D = 57}$