Number Theory and Cryptography

CHAPTER 4

SECTION 4.1, 4.3, 4.6

4.1 Divisibility and Modular Arithmetic
4.3 Primes and Greatest Common Divisor
4.6 Cryptography

The Integers & Division

Division

- Let $a,b \in \mathbf{Z}$ with $a \neq 0$.
- a|b ≡ "a divides b" if there is an integer c such that b=ac.("$\exists c(ac=b)$")
- *So:* a is a ***factor*** or a ***divisor*** of b, and b is a ***multiple*** of a.
- **a** doesn't divide **b** is denoted by **$a \nmid b$.**
  - Example: $3 \mid -12 \Leftrightarrow$ **True**, but $3 \mid 7 \Leftrightarrow$ **False**.

Divisors Examples

Q: Which of the following is true?

1. $77 \mid 7$
2. $7 \mid 77$
3. $24 \mid 24$
4. $0 \mid 24$
5. $24 \mid 0$

Divisors Examples

A:

1. 77 | 7: false bigger number can't divide smaller positive number
2. 7 | 77: true because $77 = 7 \cdot 11$
3. 24 | 24: true because $24 = 24 \cdot 1$
4. 0 | 24: false, only 0 is divisible by 0
5. 24 | 0: true, 0 is divisible by every number ($0 = 24 \cdot 0$)

Facts: The Divides Relation

- $\forall a,b,c \in \mathbf{Z}$:
  1. $(a|b \wedge a|c) \rightarrow a \mid (b + c)$
  2. $a|b \rightarrow a|bc$
  3. $(a|b \wedge b|c) \rightarrow a|c$

Examples:

1. $3|12 \wedge 3|9 \rightarrow 3|(12+9) = 3|21 = 7$
2. $2|6 \rightarrow 2|(6 \times 3) = 2|18 = 9$
3. $4|8 \wedge 8|64 \rightarrow 4|64 = 16$

Composite & Prime Numbers

- A **positive integer *p*>1** is *prime* if the only positive factors of ***p*** are 1 and *p*
  - ☻ Some **primes**: **2,3,5,7,11,13**...
- **Non-prime integers greater than 1** are called *composite*, because they can be ***composed*** by ***multiplying two integers*** greater than **1**.

Fundamental Theorem of Arithmetic

Its "Prime Factorization"

- Every positive integer greater than 1 has a unique representation as a prime or as the product of two or more primes where the prime factors are written in order of increasing size.

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$

$13 = 13$

$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Theorem

- If n is composite integer, then n has prime divisor $\leq \sqrt{n}$
- Ex: 49 → prime numbers less than $\sqrt{49}$ are 2,3,5,7

  16 → prime numbers less than $\sqrt{16}$ are 2,3

- An integer n is prime if it is not divisible by any prime $\leq \sqrt{n}$
- Ex: 13 where $\sqrt{13}$ = 3.6 so the prime numbers are 2,3 but **non of them divides** 13 so 13 is prime

Prime Factorization Technique

- To find the prime factor of an integer *n*:

1- find $\sqrt{n}$

2- list all primes $\leq \sqrt{n}$

2, 3, 5, 7,…root of *n*

3- find all prime factors that divides *n*.

Prime Factorization Examples

Exercise 1: Show that 100 is composite?

Exercise 2: Show that 101 is prime?

Exercise 3: Find the prime factors of 7007?

Ex: Show that 100 is composite?

Sol.

1) $\sqrt{100} = 10$

2) So the number may be divided by: **2, 3, 5, 7** only (all primes less than 10)

3) $2 \mid 100$ since $100/2 = 50$

∴ The number 100 is not prime, So it is composite.

Ex: Show that 101 is prime?

Sol.

1) $\sqrt{101} \approx 10$

2) So the number may be divided by: **2, 3, 5, 7** only (all primes less than 10)

3) $2 \nmid 101$ $3 \nmid 101$ $5 \nmid 101$ $7 \nmid 101$

101 is not divided by **2,3,5,7**

∴ The number 101 is prime

Ex: find the prime factors of 7007?

1) $\sqrt{7007} \approx 83$

2) So the number may be divided by: 2, 3, 5, 7, 11, 13, 17, 19 … < 83 (all primes less than 83)

3) $\frac{7007}{7} = 1001$ $\frac{1001}{7} = 143$ $\frac{143}{11} = 13$ $\frac{13}{13} = 1$

$7007 = 7 \times 7 \times 11 \times 13 = 7^2 \times 11 \times 13$

Primary Testing Example

EG: Test if **139** and **143** are primes.

List all primes up to $\sqrt{n}$ and check if they divide the numbers.

2: Neither is **even**

3: **Sum of digits trick**: 1+3+9 = 13, 1+4+3 = 8 so neither divisible by 3

5: **Don't end in 0 or 5**

7: 140 divisible by 7 so neither div. by 7

11: **Alternating sum trick**: 1-3+9 = 7 so 139 not div. by 11. 1-4+3 = 0 so **143** *is* divisible by **11**.

STOP! Next prime 13 need not be examined since bigger than $\sqrt{n}$.

Conclude: 139 is prime, 143 is composite.

Greatest Common Division (GCD)

- The *greatest common divisor* gcd(*a*,*b*) of integers *a*,*b* (not both 0) is the largest (most positive) integer *d* that is a divisor both of *a* and of *b*.

2 Ways to find GCD

1. **Find all positive common divisors of both a and b, then take the largest divisor**

Ex: find gcd (24, 36)?

Divisors of 24: 1, 2, 3, 4, 6, 8 , **12**, 24

Divisors of 36: 1, 2, 3, 4, 6, 9, **12**, 18,36

Common divisors: 1, 2, 3, 4, 6, **12**

MAXIMUM = **12**

∴ gcd (24, 36) = **12**

2. Use prime factorization: Take the min

Ex: Find $\gcd(24, 36)$

$24 = 2 \times 2 \times 2 \times 3 = 2^3 \times 3$

$36 = 2 \times 2 \times 3 \times 3 = 2^2 \times 3^2$

$\gcd(24,36) = 2^2 \times 3 = 12$

Ex: find gcd (120, 500)?

$120 = 2^3 \times 3^1 \times 5$

$500 = 2^2 \times 5^3 \times 3^0$

$\therefore$ gcd (120, 500) $= 2^2 \times 5 \times 3^0 = 20$

Greatest Common Division

EG: More realistic. Find gcd(98,420).

Find prime decomposition of each number and find all the common factors:

$98 = 2 \cdot 49 = 2 \cdot 7 \cdot 7$

$420 = 2 \cdot 210 = 2 \cdot 2 \cdot 105 = 2 \cdot 2 \cdot 3 \cdot 35$

$= 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7$

Underline common factors: $\underline{2 \cdot 7} \cdot 7, 2 \cdot \underline{2} \cdot 3 \cdot 5 \cdot \underline{7}$

Therefore, gcd(98,420) = 14

Ex: find gcd (17, 22)?

No common divisors so gcd (17, 22)=1 so the numbers 17 and 22 are called ***relatively prime.***

Greatest Common Division Relatively Prime

Q: Find the following gcd's:

1. gcd(11,77)
2. gcd(33,77)
3. gcd(24,36)
4. gcd(24,25)

Greatest Common Division Relatively Prime

A:

1. gcd(11,77) = 11
2. gcd(33,77) = 11
3. gcd(24,36) = 12
4. gcd(24,25) = 1. Therefore 24 and 25 are relatively prime.

NOTE: A prime number is relatively prime to all other numbers which it doesn't divide.

DEF: a and b are said to be ***relatively prime*** if $\gcd(a,b) = 1$, so no prime common divisors.

Least Common Multiple

- lcm(a,b) of positive integers a, b, is the smallest positive integer that is a multiple both of a and of b.

Find lcm(6,10) ? Take the max

$6 = 2 \times 3$

$10 = 2 \times 5$

$\therefore$ Lcm(6,10) $= 2 \times 3 \times 5 = 30$

Find Lcm (24, 36)?

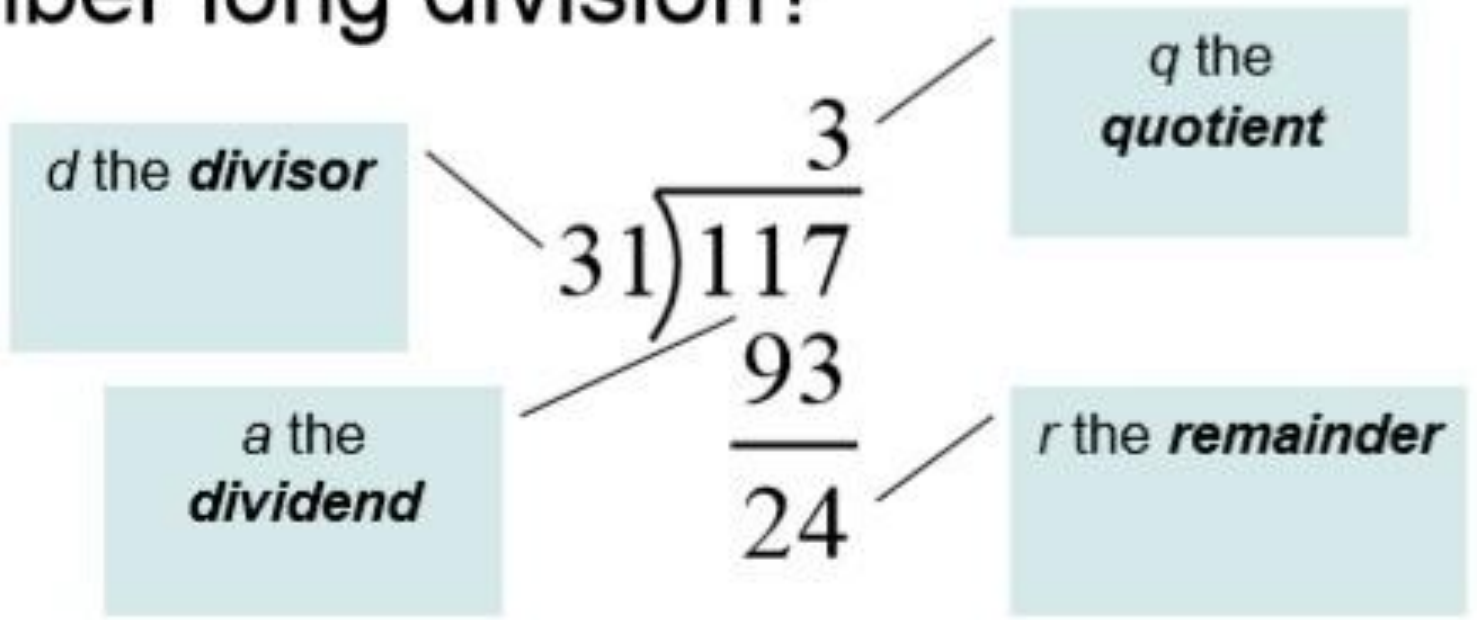
$24 = 2^3 \times 3^1$

$36 = 2^2 \times 3^2$

$\therefore$ Lcm (24, 36) $= 2^3 \times 3^2 = 72$

Division

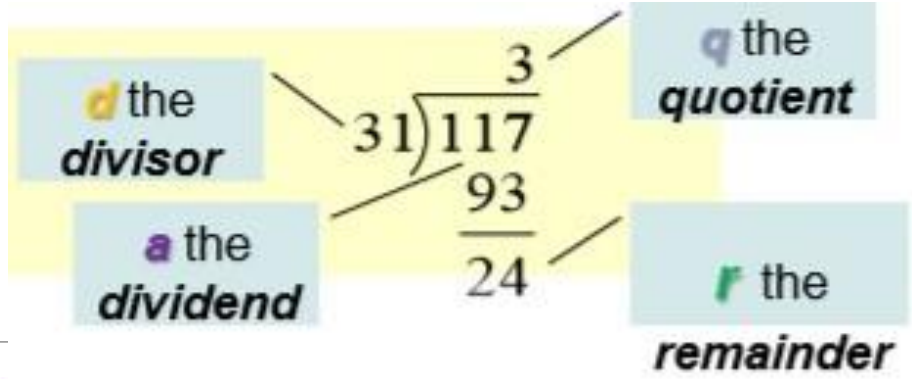
Remember long division?



$$117 = 31 \cdot 3 + 24$$

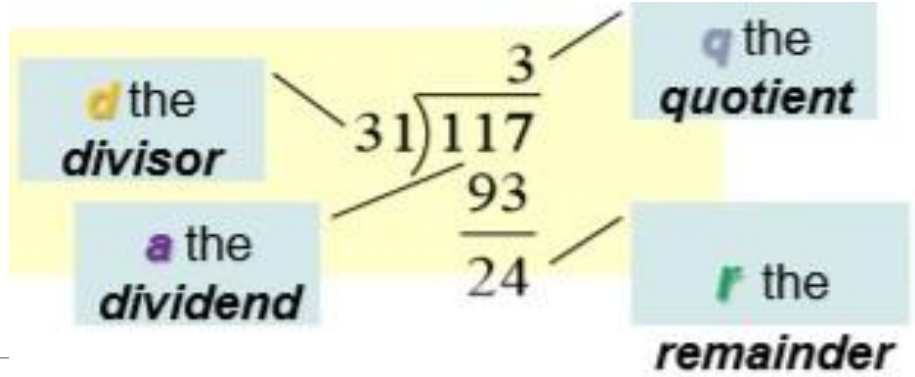
$$a = d \times q + r$$

The Division "Algorithm"



- Let **a** be an integer and **d** a positive integer, then there are unique integers **q** and **r** such that: $a = d \times q + r$, $0 \leq r < d$
- **d** is called **divisor**, and **a** is called **dividend**
- **q** is the **quotient**, and **r** is the **remainder** (positive integer)
- $q = a \text{ div } d$, $r = a \bmod d$

Examples



What are the quotient and remainder when 101 is divided by 11?

- What are the **quotient** and the **remainder** when **-11** is divided by **3?**

Solutions

$101 = 11 \times 9 + 2$, $q = 9, r = 2$

$a = d \times q + r, \quad 0 \leq r < d$

$-11 = 3 \times (-4) + 1$,$q = -4, r = 1$

Note: $-11 \neq 3 \times (-3) - 2$ because $r \geq 0$

(can't be negative)

mod Function Start Here

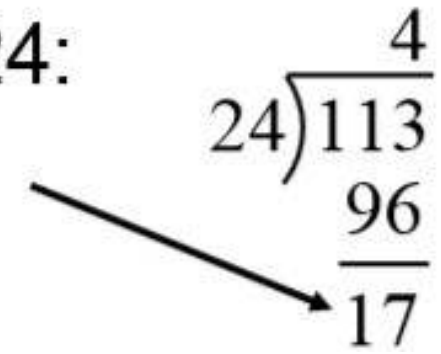
A: Compute

1. 113 **mod** 24: $24\overline{)113}$

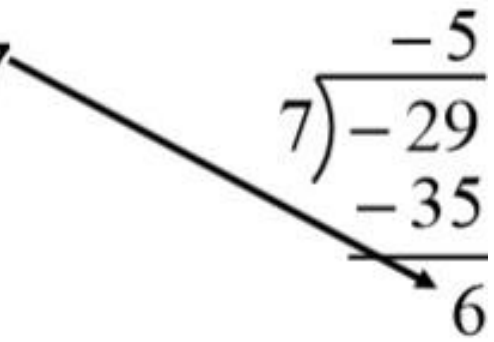
2. -29 **mod** 7 $7\overline{)-29}$

mod Function

1. 113 **mod** 24:



2. -29 **mod** 7



Question

- What time it will be (on a 24-hour clock) 50 hours from 11 am?

- After 24 hours it will be 11 am
- After another 24 hours it will be 11 am
  - This is after 48 hours
- After 2 more hours it will be 13 (1 pm)!
  - This is after 50 hours

- Is there another way?

Question

- What time it will be (on a 24-hour clock) 50 hours from 11 am?
  - Calculate (11 + 50) mod 24?
- We can also use mod Function to convert time from 24-hour clock to 12-hour clock
- Calculate 13 mod 12?
- Calculate 23 mod 12?

Modular Congruence

Let $a, b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$.

Thm:

a is congruent to b modulo m

written "$a \equiv b \pmod{m}$", iff

1) $a \bmod m = b \bmod m$
2) $m \mid a-b$ ***i.e.*** $(a-b) \bmod m = 0$.

"$a \equiv b \pmod m$", iff
1) **$a \bmod m = b \bmod m$**
2) **$m \mid a-b$** **i.e.** $(a-b) \bmod m = 0$.

Examples

Is 17 congruent to 5 modulo 6 ?

$17 \bmod 6 = 5$ and $5 \bmod 6 = 5$

and $6 \mid (17-5) \leftrightarrow 6 \mid 12$ where 12/6= 2

Then $17 \equiv 5 \pmod 6$

Is 24 congruent to 14 modulo 6?

Since, $24 \bmod 6 = 0$ ***and*** $14 \bmod 6 = 2$

Then, $24 \not\equiv 14 \pmod 6$ ***and*** $6 \nmid (24-14) \leftrightarrow 6 \nmid 10$

Useful Congruence Theorems

- Let $a,b,c,d \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:
  - $a+c \equiv b+d \pmod{m}$, and
  - $ac \equiv bd \pmod{m}$

Ex.:

let $7 \equiv 2 \pmod 5$ and

$11 \equiv 1 \pmod 5$

Then:

$(7 + 11) \equiv (2 + 1) \pmod 5 \leftrightarrow 18 \equiv 3 \pmod 5$

and

$(7 \times 11) \equiv (2 \times 1) \pmod 5 \leftrightarrow 77 \equiv 2 \pmod 5$



4.6 Cryptography

Section Summary

Classical Cryptography

Cryptosystems

Public Key Cryptography

RSA Cryptosystem

Cryptographic Protocols

Primitive Roots and Discrete Logarithms

Why Cryptography

Cryptography is a science that applies complex mathematics and logic to design strong encryption methods.

Cryptography is also an art.

Cryptography allows people to keep confidence in the electronic world.

People can do their business on electric channel without worrying of deceit and deception.

Symmetric Encryption (single-key encryption)

Symmetric Encryption

The universal technique for providing confidentiality



also referred to as single-key encryption

Algorithms: DES, Triple DES, and AES

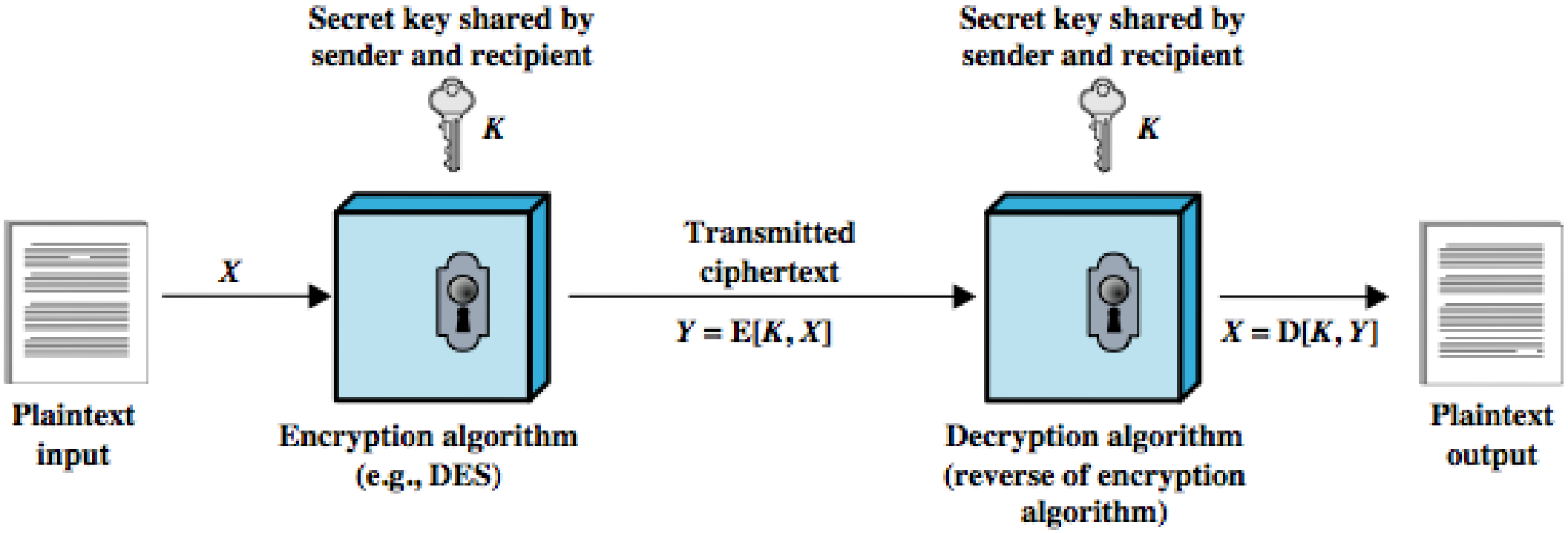


Two requirements for secure use:

- need a strong encryption algorithm
- **sender** and **receiver** must have obtained copies of the **secret key** in a secure fashion
  - and must keep the key secure



Symmetric Encryption



Caesar Cipher

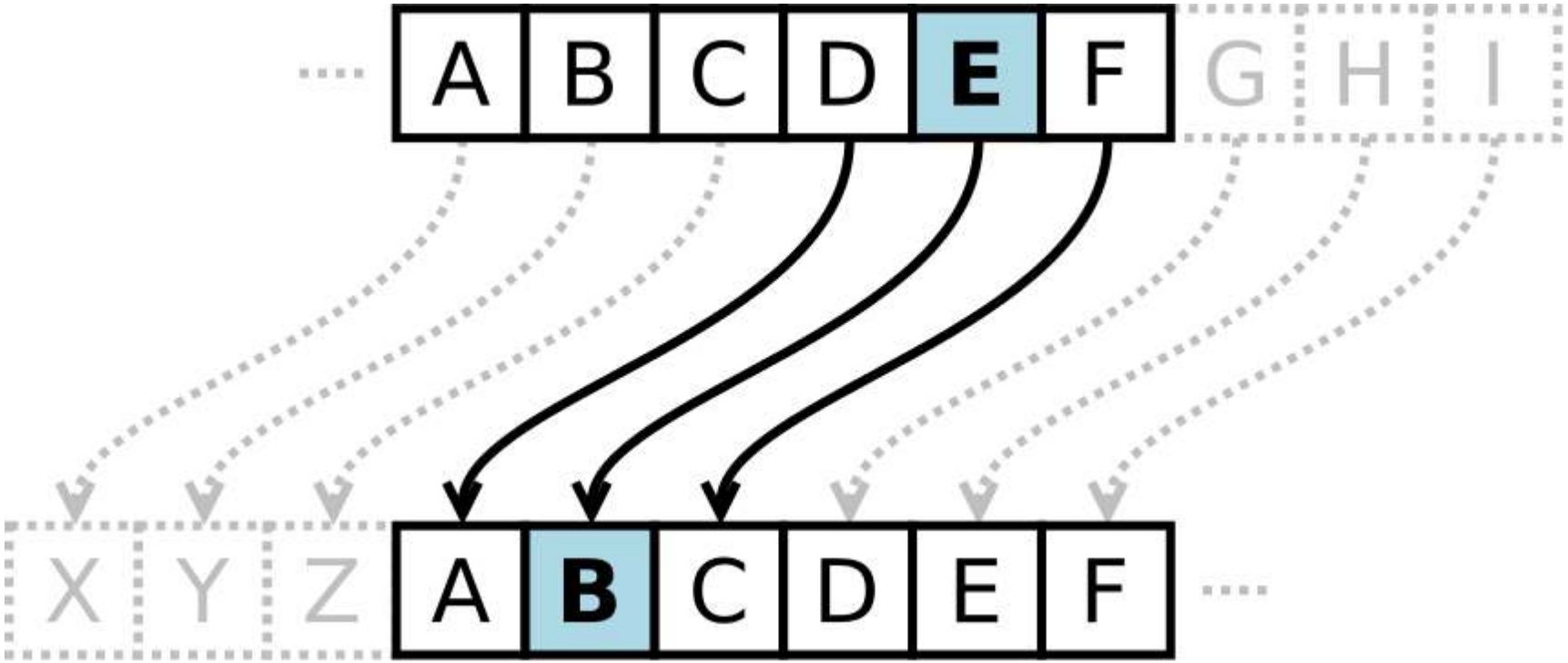


- Julius Caesar created secret messages by shifting each letter three letters forward in the alphabet (sending the last three letters to the first three letters.)
- For example, the letter B is replaced by E and the letter X is replaced by A. This process of making a message secret is an example of *encryption*.

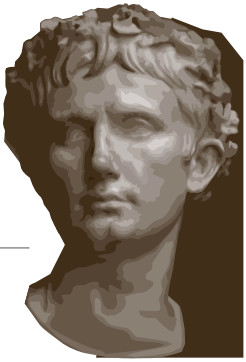
- Here is how the encryption process works:
  - Replace each letter by an integer from $\mathbf{Z}_{26}$, that is an integer from 0 to 25 representing one less than its position in the alphabet.
  - The encryption function is $f(p) = (p + 3) \bmod 26$. It replaces each integer p in the set $\{0,1,2,\ldots,25\}$ by $f(p)$ in the set $\{0,1,2,\ldots,25\}$.
  - Replace each integer p by the letter with the position $p + 1$ in the alphabet.

Caesar cipher





Caesar Cipher



Example: Encrypt the message “MEET YOU IN THE PARK” using the Caesar cipher.

Solution: $12\ 4\ 4\ 19 \quad 24\ 14\ 20 \quad 8\ 13 \quad 19\ 7\ 4 \quad 15\ 0\ 17\ 10.$

Now replace each of these numbers p by $f(p) = (p + 3)$ **mod** 26.

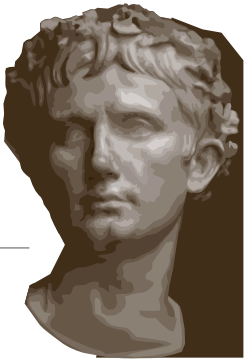
$$15\ 7\ 7\ 22 \quad 1\ 17\ 23 \quad 11\ 16 \quad 22\ 10\ 7 \quad 18\ 3\ 20\ 13.$$

Translating the numbers back to letters produces the encrypted message

“PHHW BRX LQ WKH SDUN.”

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Caesar Cipher



To recover the original message, use $f^{-1}(p) = (p-3) \bmod 26$. So, each letter in the coded message is shifted back three letters in the alphabet, with the first three letters sent to the last three letters. This process of recovering the original message from the encrypted message is called *decryption*.

The Caesar cipher is one of a family of ciphers called *shift ciphers*. Letters can be shifted by an integer k, with 3 being just one possibility. The encryption function is

$$f(p) = (p + k) \bmod 26$$

and the decryption function is

$$f^{-1}(p) = (p-k) \bmod 26$$

The integer k is called a *key*.

Shift Cipher

Example 1: Encrypt the message "STOP GLOBAL WARMING" using the shift cipher with $k = 11$.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Shift Cipher

Example 1: Encrypt the message "STOP GLOBAL WARMING" using the shift cipher with $k = 11$.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

$$18\ 19\ 14\ 15 \quad 6\ 11\ 14\ 1\ 0\ 11 \quad 22\ 0\ 17\ 12\ 8\ 13\ 6.$$

Apply the shift $f(p) = (p + 11)$ **mod** 26, yielding

$$3\ 4\ 25\ 0 \quad 17\ 22\ 25\ 12\ 11\ 22 \quad 7\ 11\ 2\ 23\ 19\ 24\ 17.$$

Translating the numbers back to letters produces the ciphertext

"DEZA RWZMLW HLCXTYR."

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Shift Cipher

Example 2: Decrypt the message "LEWLYPLUJL PZ H NYLHA ALHJOLY" that was encrypted using the shift cipher with $k = 7$.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Shift Cipher

Example 2: Decrypt the message "LEWLYPLUJL PZ H NYLHA ALHJOLY" that was encrypted using the shift cipher with ***k* = 7**.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

$$11\ 4\ 22\ 11\ 24\ 15\ 11\ 20\ 9\ 11 \quad 15\ 25 \quad 7 \quad 13\ 24\ 11\ 7 \quad 0 \quad 0\ 11\ 7 \quad 9 \quad 14 \quad 11 \quad 24.$$

Shift each of the numbers by $-k = -7$ modulo 26, yielding

$$4\ 23\ 15\ 4\ 17\ 8\ 4\ 13\ 2\ 4 \quad 8\ 18 \quad 0 \quad 6\ 17\ 4 \quad 0 \quad 19 \quad 19 \quad 4 \quad 0 \quad 2 \quad 7 \quad 4 \quad 17.$$

Translating the numbers back to letters produces the decrypted message

"EXPERIENCE IS A GREAT TEACHER."

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Affine Ciphers

Shift ciphers are a special case of *affine ciphers* which use functions of the form $f(p) = (ap + b) \bmod 26$,

where a and b are integers, chosen so that f is a bijection.

The function is a bijection if and only if $\gcd(a,26) = 1$.

Example: What letter replaces the letter K when the function $f(p) = (7p + 3) \bmod 26$ is used for encryption.

Solution: Since 10 represents K, $f(10) = (7 \cdot 10 + 3) \bmod 26 = 21$, which is then replaced by V.

To decrypt a message encrypted by a shift cipher, the congruence $c \equiv ap + b \pmod{26}$ needs to be solved for p.

- Subtract b from both sides to obtain $c - b \equiv ap \pmod{26}$.
- Multiply both sides by the inverse of a modulo 26, which exists since $\gcd(a,26) = 1$.
- $\bar{a}(c - b) \equiv \bar{a}ap \pmod{26}$, which simplifies to $\bar{a}(c - b) \equiv p \pmod{26}$.
- $p \equiv \bar{a}(c - b) \pmod{26}$ is used to determine p in $\mathbf{Z}_{26}$.

Cryptanalysis of Affine Ciphers

The process of recovering plaintext from ciphertext without knowledge both of the encryption method and the key is known as *cryptanalysis* or *breaking codes*.

An important tool for cryptanalyzing ciphertext produced with a affine ciphers is the relative frequencies of letters. The nine most common letters in the English texts are E 13%, T 9%, A 8%, O 8%, I 7%, N 7%, S 7%, H 6%, and R 6%.

To analyze ciphertext:

- Find the frequency of the letters in the ciphertext.
- Hypothesize that the most frequent letter is produced by encrypting E.
- If the value of the shift from E to the most frequent letter is k, shift the ciphertext by $-k$ and see if it makes sense.
- If not, try T as a hypothesis and continue.

Example: We intercepted the message "ZNK KGXRE HOXJ MKZY ZNK CUXS" that we know was produced by a shift cipher. Let's try to cryptanalyze.

Solution: The most common letter in the ciphertext is K. So perhaps the letters were shifted by 6 since this would then map E to K. Shifting the entire message by -6 gives us "THE EARLY BIRD GETS THE WORM."

Cryptosystems

Definition: A *cryptosystem* is a five-tuple (P,C,K,E,D), where

- P is the set of plainntext strings,
- C is the set of ciphertext strings,
- K is the *keyspace* (set of all possible keys),
- E is the set of encryption functions, and
- D is the set of decryption functions.

The encryption function in E corresponding to the key k is denoted by E_k and the decryption function in D that decrypts cipher text encrypted using E_k is denoted by D_k. Therefore:

$$D_k(E_k(p)) = p, \text{ for all plaintext strings } p.$$

Cryptosystems

Example: Describe the family of shift ciphers as a cryptosystem.

Solution: Assume the messages are strings consisting of elements in $\mathbf{Z}_{26}$.

- P is the set of strings of elements in $\mathbf{Z}_{26}$,
- C is the set of strings of elements in $\mathbf{Z}_{26}$,
- K = $\mathbf{Z}_{26}$,
- E consists of functions of the form

$E_k(p) = (p + k) \bmod 26$, and

- D is the same as E where $D_k(p) = (p - k) \bmod 26$.

Public Key Cryptography

Public Key Cryptography

All classical ciphers, including shift and affine ciphers, are *private key cryptosystems*. Knowing the encryption key allows one to quickly determine the decryption key.

All parties who wish to communicate using a private key cryptosystem must share the key and keep it a secret.

In **public key cryptosystems**, first invented in the 1970s, knowing how to encrypt a message does not help one to decrypt the message. Therefore, everyone can have a publicly known encryption key. The only key that needs to be kept secret is the decryption key.

The RSA Cryptosystem



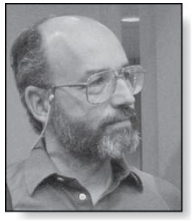
Clifford Cocks
(Born 1950)

A public key cryptosystem, now known as the RSA system was introduced in 1976 by three researchers at MIT.

Ronald Rivest
(Born 1948)



Adi Shamir
(Born 1952)



Leonard
Adelman
(Born 1945)



It is now known that the method was discovered earlier by Clifford Cocks, working secretly for the UK government.

The RSA Cryptosystem

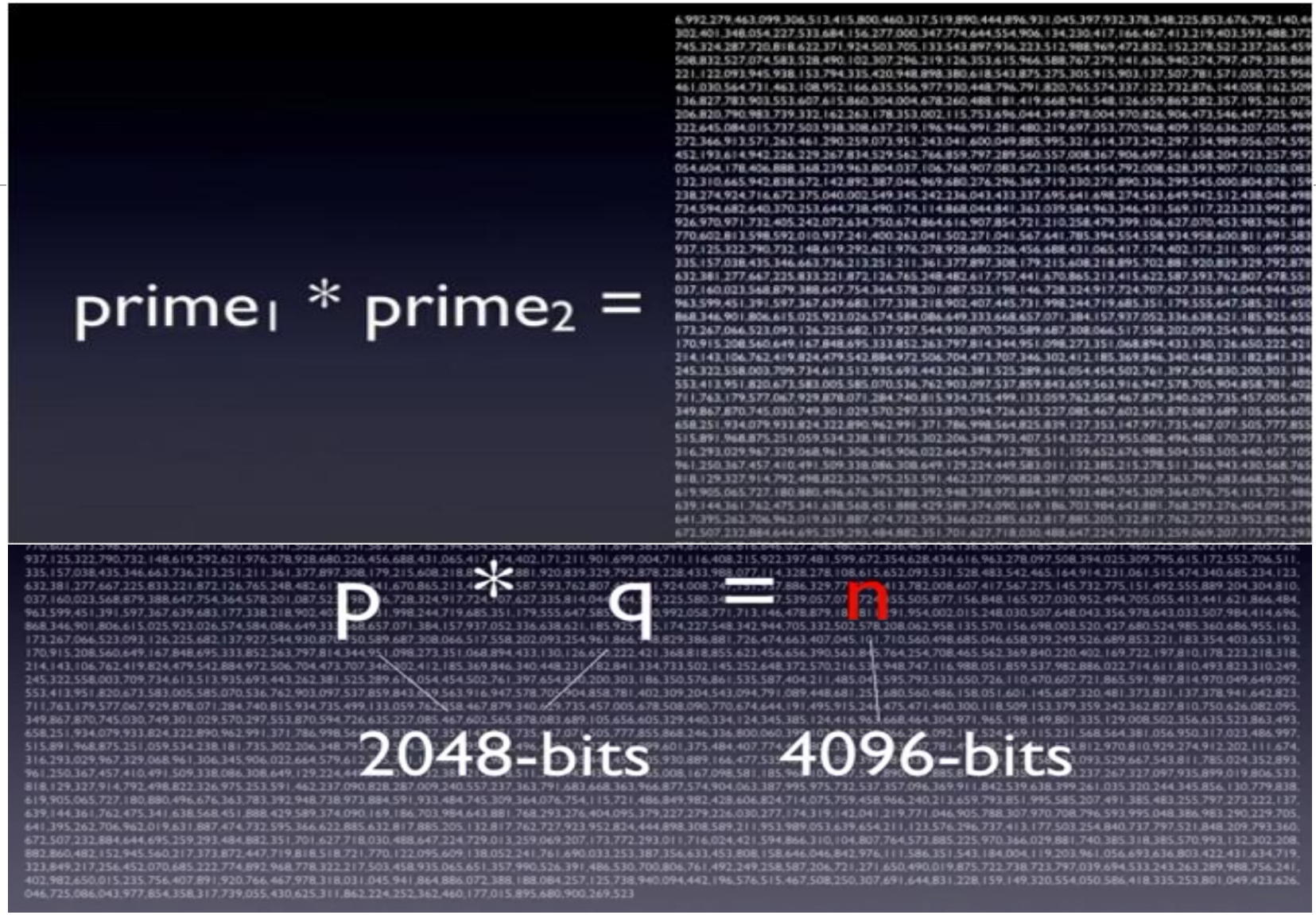
The RSA algorithm involves **four steps**: key generation, key distribution, encryption and decryption.

The public encryption key is (n,e), where $n = pq$, the modulus is the product of two large primes p and q ,say with 200 digits each, and an exponent e that is relatively prime to $(p-1)(q-1)$.

The two large primes can be quickly found using probabilistic primarily tests, discussed earlier.

But $n = pq$, with approximately 400 digits, cannot be factored in a reasonable length of time.


6,992,279,463,099,306,513,415,800,460,317,519,890,444,896,931,045,397,932,378,348,225,853,676,792,140,441,678,927,628,875,456,695,024,506,006,332,626,365,194,962,240,453,639,352,597,632,032,589,188,462,141,
302,401,348,054,227,533,684,156,277,000,347,774,644,554,906,134,230,417,166,467,413,219,403,593,488,372,312,125,203,442,390,298,437,403,577,853,111,194,194,073,337,193,245,842,621,737,450,434,520,258,048,764,
745,324,287,720,818,622,371,924,503,705,133,543,897,936,223,512,988,969,472,832,152,278,521,237,265,459,888,516,313,452,283,340,922,585,409,923,962,202,001,816,710,554,500,547,973,295,462,450,900,608,383,198,
508,832,527,074,583,528,490,102,307,296,219,126,353,615,966,588,767,279,141,636,940,274,797,479,338,868,467,577,077,040,185,880,809,961,493,697,372,739,274,506,389,327,661,112,796,594,243,231,999,751,065,698,
221,122,093,945,938,153,794,335,420,948,898,380,618,543,875,275,305,915,903,137,507,781,571,030,725,956,338,741,630,099,402,346,557,511,395,955,348,213,164,544,819,539,861,611,260,066,779,617,072,171,274,236,
461,030,564,731,463,108,952,166,635,556,977,930,448,796,791,820,765,574,337,122,732,876,144,058,162,509,032,085,106,169,921,171,363,010,570,638,293,420,474,748,175,986,407,672,409,709,462,572,398,469,885,241,
136,827,783,903,553,607,615,860,304,004,678,260,488,181,419,668,941,548,126,659,869,282,357,195,261,075,765,993,158,569,755,459,695,855,779,838,519,150,400,678,997,539,754,753,620,115,891,706,483,333,102,727,
206,820,790,983,739,332,162,263,178,353,002,115,753,696,044,349,878,004,970,826,906,473,546,447,725,969,053,184,165,630,677,823,331,554,853,520,484,365,563,312,156,265,512,027,972,704,000,165,273,017,881,629,
322,645,084,015,737,503,938,308,637,219,196,946,991,281,480,219,697,353,770,968,409,150,636,207,505,499,687,872,610,706,551,662,688,369,435,010,005,223,929,553,909,894,961,694,936,984,813,150,984,853,928,733,
272,366,913,571,263,461,290,259,073,951,243,041,600,049,885,995,321,614,373,242,297,134,989,056,074,595,082,131,009,422,067,878,401,611,809,257,511,079,036,596,391,474,216,913,825,691,851,756,406,458,900,992,
452,193,614,942,226,229,267,834,529,562,766,859,797,289,560,557,008,367,906,697,561,658,204,923,257,957,542,893,608,902,316,867,574,460,647,152,207,143,506,972,269,723,597,269,684,792,602,430,424,412,803,728,
054,604,178,406,888,368,239,963,804,037,106,768,907,083,672,310,454,454,792,008,628,393,907,710,028,083,119,995,325,741,245,920,841,554,066,652,003,426,067,996,837,873,407,896,266,077,611,609,051,779,846,331,
132,310,665,942,838,672,142,892,387,046,969,680,276,296,369,719,330,271,890,336,299,545,000,804,876,159,738,728,851,140,778,102,381,072,526,544,481,501,722,189,148,758,458,147,824,387,259,572,079,408,550,505,
238,274,924,716,672,375,040,002,549,345,242,236,043,433,337,695,641,698,274,563,649,942,512,438,048,498,391,050,111,851,547,399,464,335,386,792,446,609,740,527,942,408,022,732,291,158,534,380,782,984,874,903,
734,594,682,640,370,253,644,738,490,174,114,868,044,841,363,039,584,963,346,431,569,117,223,233,992,891,032,375,459,679,726,017,306,363,948,847,311,296,864,664,829,582,413,242,829,254,966,415,059,452,814,265,
926,970,971,732,405,242,072,634,750,674,864,616,907,854,721,210,258,479,399,106,627,070,453,983,965,184,629,115,543,773,566,649,119,197,756,815,739,961,943,358,317,191,643,930,811,985,869,594,980,508,532,594,
770,602,813,598,592,010,937,241,400,263,041,502,271,041,567,641,785,394,554,558,934,958,600,811,691,583,044,870,056,816,646,027,246,480,517,336,467,156,136,550,764,185,309,202,071,460,225,586,921,971,205,726,
937,125,322,790,732,148,619,292,621,976,278,928,680,226,456,688,431,065,417,174,402,171,211,901,699,004,711,116,408,215,922,397,481,599,672,354,628,434,616,963,278,097,508,394,025,309,795,615,172,552,706,511,
335,157,038,435,346,663,736,213,251,211,361,377,897,308,179,215,608,218,895,702,881,920,839,329,792,878,228,433,988,077,114,328,278,108,615,652,093,531,528,483,542,465,164,914,231,061,515,474,340,685,234,123,
632,381,277,667,225,833,221,872,126,765,248,482,617,757,441,670,865,213,415,622,587,593,762,807,478,551,924,008,747,151,937,886,329,773,908,413,782,008,607,417,567,275,145,732,775,151,492,555,889,204,304,810,
037,160,023,568,879,388,647,754,364,578,201,087,523,198,146,728,324,917,724,707,627,335,814,044,944,509,225,580,348,611,677,539,057,072,724,455,505,877,156,848,165,927,030,952,494,705,055,413,441,621,866,484,
963,599,451,391,597,367,639,683,177,338,218,902,407,445,731,998,244,719,685,351,179,555,647,585,211,450,992,058,771,713,146,478,879,188,811,291,954,002,015,248,030,507,648,043,356,978,643,033,507,984,414,696,
868,346,901,806,615,025,923,026,574,584,086,649,333,668,657,071,384,157,937,052,336,638,621,185,925,655,174,227,548,342,944,705,332,502,578,208,062,958,135,570,156,698,003,520,427,680,524,985,360,686,955,163,
173,267,066,523,093,126,225,682,137,927,544,930,870,750,589,687,308,066,517,558,202,093,254,961,866,948,829,386,881,726,474,663,407,045,101,710,560,498,685,046,658,939,249,526,689,853,221,183,354,403,653,193,
170,915,208,560,649,167,848,695,333,852,263,797,814,344,951,098,273,351,068,894,433,130,126,650,222,421,368,818,855,623,456,656,390,563,845,764,254,708,465,562,369,840,220,402,169,722,197,810,178,223,218,318,
214,143,106,762,419,824,479,542,884,972,506,704,473,707,346,302,412,185,369,846,340,448,231,182,841,334,733,502,145,252,648,372,570,216,534,948,747,116,988,051,859,537,982,886,022,714,611,810,493,823,310,249,
245,322,558,003,709,734,613,513,935,693,443,262,381,525,289,616,054,454,502,761,397,654,830,200,303,186,350,576,861,535,587,404,211,485,045,595,793,533,650,726,110,470,607,721,865,591,987,814,970,049,649,092,
553,413,951,820,673,583,005,585,070,536,762,903,097,537,859,843,659,563,916,947,578,705,904,858,781,402,309,204,543,094,791,089,448,681,252,680,560,486,158,051,601,145,687,320,481,373,831,137,378,941,642,823,
711,763,179,577,067,929,878,071,284,740,815,934,735,499,133,059,762,858,467,879,340,629,735,457,005,678,508,090,770,674,644,191,495,915,246,475,471,440,300,118,509,153,379,359,242,362,827,810,750,626,082,095,
349,867,870,745,030,749,301,029,570,297,553,870,594,726,635,227,085,467,602,565,878,083,689,105,656,605,329,440,334,124,345,385,124,416,963,668,464,304,971,965,198,149,801,335,129,008,502,356,635,523,863,493,
658,251,934,079,933,824,322,890,962,991,371,786,998,564,825,839,127,353,147,971,735,467,071,505,777,855,868,246,336,800,060,399,102,768,528,066,286,092,157,524,569,115,231,568,564,381,056,950,317,023,486,997,
515,891,968,875,251,059,534,238,181,735,302,206,348,793,407,514,322,723,955,082,496,488,170,273,175,999,601,375,484,407,774,409,802,353,059,463,407,781,497,982,813,061,533,812,970,810,929,274,912,202,111,674,
316,293,029,967,329,068,961,306,345,906,022,664,579,612,785,311,159,652,676,988,504,553,505,440,457,105,930,889,166,477,535,457,928,862,396,584,339,446,112,789,912,758,223,093,529,667,543,811,785,024,352,893,
961,250,367,457,410,491,509,338,086,308,649,129,224,449,583,011,132,385,215,278,511,366,943,430,568,765,008,167,098,581,185,968,103,707,597,890,727,885,871,453,835,744,660,237,267,327,097,935,899,019,806,533,
818,129,327,914,792,498,822,326,975,253,591,462,237,090,828,287,009,240,557,237,363,791,683,668,363,966,877,574,904,063,387,995,975,732,537,357,096,369,911,842,539,638,399,261,035,320,244,345,856,130,779,838,
619,905,065,727,180,880,496,676,363,783,392,948,738,973,884,591,933,484,745,309,364,076,754,115,721,486,849,982,428,606,824,714,075,759,458,966,240,213,659,793,851,995,585,207,491,385,483,255,797,273,222,137,
639,144,361,762,475,341,638,568,451,888,429,589,374,090,169,186,703,984,643,881,768,293,276,404,095,379,227,279,226,030,277,174,319,142,041,219,771,046,905,788,307,970,708,796,593,995,048,386,983,290,229,705,
641,395,262,706,962,019,631,887,474,732,595,366,622,885,632,817,885,205,132,817,762,727,923,952,824,444,898,308,589,211,953,989,053,639,654,211,123,576,296,737,413,177,503,254,840,737,797,521,848,209,793,360,
672,507,232,884,644,695,259,293,484,882,351,701,627,718,030,488,647,224,729,013,259,069,207,173,772,293,011,716,024,421,594,866,310,104,807,764,573,885,225,970,366,029,881,740,385,318,385,570,993,132,302,208,
882,860,482,152,945,560,217,373,872,447,719,818,518,721,770,122,095,609,138,052,241,761,690,033,253,387,356,633,453,808,158,646,046,842,976,111,586,351,543,184,004,119,203,961,056,693,636,803,422,431,634,719,
323,849,217,256,452,070,685,222,774,892,968,778,322,217,503,458,935,065,651,357,990,526,391,486,530,700,806,761,492,249,258,587,206,721,271,650,490,019,875,722,738,723,797,039,694,533,243,263,289,988,756,241,
402,982,650,015,235,756,407,891,920,766,467,978,318,031,045,941,864,886,072,388,188,084,257,125,738,940,094,442,196,576,515,467,508,250,307,691,644,831,228,159,149,320,554,050,586,418,335,253,801,049,423,626,
046,725,086,043,977,854,358,317,739,055,430,625,311,862,224,252,362,460,177,015,895,680,900,269,523


prime1 * prime2 =
p * q = n
2048-bits
4096-bits

The RSA Cryptosystem

Step-1: Select two prime numbers p and q where $p \neq q$.

Step-2: Calculate $n = p * q$.

Step-3: Calculate $\Phi(n) = (p-1) * (q-1)$.

Step

-4: Select e such that, e is relatively prime to $\Phi(n)$, i.e. $(e, \Phi(n)) = 1$ and $1 < e < \Phi(n)$

Step-5: Calculate $d = e^{-1} \bmod \Phi(n)$ or $ed = 1 \bmod \Phi(n)$.

Step-6: Public key = {e, n}, private key = {d, n}.

Step-7: Find out cipher text using the formula,

$C = P^e \bmod n$ where, $P < n$ where C = Cipher text, P = Plain text, e = Encryption key and n=block size.

Step-8: $P = C^d \bmod n$. Plain text P can be obtain using the given formula. where, d =decryption key

RSA algorithm explanation -step by step example

Step – 1: Select two prime numbers p and q where $p \neq q$.

Example, Two prime numbers p = 13, q = 11.

Step – 2: Calculate n = p * q.

Example, n = p * q = 13 * 11 = 143.

Step – 3: Calculate $\Phi(n) = (p-1) * (q-1)$.

Example, $\Phi(n) = (13 - 1) * (11 - 1) = 12 * 10 = 120$.

Step – 4: Select **e** such that,

1- coprime with **n** and **Φ(n)**, i.e. $(e, \Phi(n)) = 1$ and

2- $1 < e < \Phi(n)$.

Example, Select e = 13, gcd (13, 120) = 1.

Continue…

Step – 5: Calculate $d = e^{-1} \bmod \Phi(n)$ or $e * d = 1 \bmod \Phi(n)$

Example, Finding d: $e * d \bmod \Phi(n) = 1$

$13 * d \bmod 120 = 1$

(How to find: $d * e = 1 \bmod \Phi(n)$ ➔ $d = ((\Phi(n) * i) + 1) / e$

$d = (120 + 1) / 13 = 9.30$ (∵ i = 1)

$d = (240 + 1) / 13 = 18.53$ (∵ i = 2)

$d = (360 + 1) / 13 = 27.76$ (∵ i = 3)

$d = (480 + 1) / 13 = 37$ (∵ i = 4))

Continue…

Step – 6: Public key = {e, n}, private key = {d, n}.

Example, Public key = {13, 143} and private key = {37, 143}.

Step – 7: Find out *cipher text* **C** using the formula, **$C = P^e \bmod n$** where, P < n.

Encryption Example, Plain text **P** = 13. (Where, P < n)

$C = P^e \bmod n = 13^{13} \bmod 143 = 52$.

Step – 8: **$P = C^d \bmod n$**. Plain text P can be obtain using the given formula.

Decryption Example, Cipher text C = 52

$P = C^d \bmod n = 52^{37} \bmod 143 = 13$.

Example

Encrypt (**$C = P^e \bmod n$**) the message B using the RSA cryptosystem with key (5,14):

$2^5 \bmod 14 = 32 \bmod 14 = 4$

4 ➔ D

Decrypt (**$P = C^d \bmod n$**) the cipher text D using the RSA cryptosystem with key (11,14):

$4^{11} \bmod 14 = 4194304 \bmod 14 \approx 2$

2➔ B

RSA Encryption

To encrypt a message using RSA using a key (n,e) :

1. Translate the plaintext message M into sequences of two digit integers representing the letters. Use 00 for A, 01 for B, … 25 for Z.
2. Concatenate the two digit integers into strings of digits.
3. Divide this string into equally sized blocks of $2N$ digits (N = number of letters in the block) where $2N$ is the largest even number $2525\ldots25$ with $2N$ digits that does not exceed n.
4. The plaintext message M is now a sequence of integers $m_1, m_2, \ldots, m_k$.
5. Each block (an integer) is encrypted using the function $C = M^e \bmod n$.

RSA Encryption- example

Example: Encrypt the message STOP using the RSA cryptosystem with key(2537,13).

- $2537 = 43 \cdot 59$,
- $p = 43$ and $q = 59$ are primes and $\gcd(e,(p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$.

Solution: Translate the letters in STOP to their numerical equivalents 18 19 14 15.

- Divide into blocks of four digits (because $2525 < n=2537 < 252525$) to obtain 1819 1415.
- Encrypt each block using the mapping $C = M^{13} \bmod 2537$.
- Since $1819^{13} \bmod 2537 = 2081$ and $1415^{13} \bmod 2537 = 2182$, the encrypted message is 2081 2182.

RSA Decryption

To decrypt a RSA ciphertext message, the decryption key d, an inverse of e modulo $(p-1)(q-1)$ is needed. The inverse exists since $\mathbf{gcd}(e,(p-1)(q-1)) = 1$.

Note that if $de \equiv 1 \pmod{(p-1)(q-1)}$, there is an integer k such that

$$de = 1 + k(p-1)(q-1).$$

With the decryption key d, we can decrypt each block with the computation $M = C^d \bmod p \cdot q$. (*see text for full derivation*)

RSA works as a public key system since the only known method of finding d is based on a factorization of n into primes. There is currently *no known feasible method for factoring large numbers into primes.*

RSA Decryption- example

Example: The message $0981\ 0461$ is received. What is the decrypted message if it was encrypted using the RSA cipher from the previous example.

Solution: The message was encrypted with $n = 43 \cdot 59 = 2537$ and exponent 13. An inverse of 13 modulo $42 \cdot 58 = 2436$ (*exercise* 2 *in Section* 4.4) is $d = 937$.

- To decrypt a block C, $M = C^{937} \bmod 2537$.
- Since $0981^{937} \bmod 2537 = 0704$ and $0461^{937} \bmod 2537 = 1115$, the decrypted message is 0704 1115. Translating back to English letters, the message is HELP.
- Here is a link to RSA calculator: https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html

Exercise - 1

Question: P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then what will be cipher text value according to RSA algorithm? Again calculate plain text value from cipher text.

Exercise - 1

Question: P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then what will be cipher text value according to RSA algorithm? Again calculate plain text value from cipher text.

Solution:

1. Two prime numbers P=7, Q=17
2. $n = P * Q = 17 * 7 = 119$ **n = 119**
3. $\Phi(n) = (P-1) * (Q-1) = (17 - 1) * (7 - 1) = 16 * 6 = 96$ **Φ(n) = 96**
4. Public key E = 5. **E= 5**
5. Calculate d = 77. $d = ((\Phi(n) * i) + 1) / e$ **d= 77**

   $d = ((96*1)+1) / 5 = 19.4$

   $d = ((96*2)+1) / 5 = 38.6$

   $d = ((96*3)+1) / 5 = 57.8$

   $d = ((96*4)+1) / 5 = 77$ (Stop finding d because getting integer value)
6. Public key = {e, n} = {5, 119}, private key = {d, n} = {77, 119}.
7. Plain text PT = 6, $CT = PT^E \bmod n = 6^5 \bmod 119 = 41$. **Cipher Text = 41**
8. Cipher text CT = 41, $PT = CT^d \bmod n = 41^{77} \bmod 119 = 6$. **Plain Text = 6**

Exercise - 2

Question: In a public key cryptosystem using RSA algorithm, user uses two prime numbers 5 and 7. He chooses 11 as Encryption key, find out decryption key. What will be the cipher text, if the plaintext is 2? Decrypt the cipher text, what will be the value of plain text?

Solution:

1. Two prime numbers p = 5, q = 7
2. n = p * q = 5 * 7 = 35 **n = 35**
3. $\Phi(n) = (p-1) * (q-1) = (5-1) * (7-1) = 4 * 6 = 24$ **$\Phi(n) = 24$**
4. Public key e = 11. **e= 11**
5. Calculate d = 11. $d = ((\Phi(n) * i) + 1) / e$ **d= 11**
6. Public key = {e, n} = {11, 35}, private key = {d, n} = {11, 35}.
7. Plain text P = 2, $C = P^e \bmod n = 2^{11} \bmod 35 = 18$. **Cipher Text = 18**
8. Cipher text C = 18, $P = C^d \bmod n = 18^{11} \bmod 35 = 2$. **Plain Text = 2**

Exercise - 3

Question: P and Q are two prime numbers. P=17, and Q=11. Take public key E=7. If plain text value is 5, then what will be cipher text value & private key value according to RSA algorithm? Again calculate plain text value from cipher text.

Solution:

1. Two prime numbers p = 17, q = 11
2. n = p * q = 17 * 11 = 187 **n = 187**
3. $\Phi(n) = (p-1) * (q-1) = (17 - 1) * (11 - 1) = 16 * 10 = 160$ **$\Phi(n) = 160$**
4. Public key e = 7. **e= 7**
5. Calculate d = 23. $d = ((\Phi(n) * i) + 1) / e$ **d= 23**
6. Public key = {e, n} = {7, 187}, private key = {d, n} = {23, 187}.
7. Plain text P = 5, $C = P^e \bmod n = 5^7 \bmod 187 = 146$. **Cipher Text = 146**
8. Cipher text C = 146, $P = C^d \bmod n = 146^{23} \bmod 187 = 5$. **Plain Text = 5**

Exercise - 4

Question: P and Q are two prime numbers. P=3, and Q=11. Take public key E=3. If original message is 00111011, then what will be cipher text value & private key value according to RSA algorithm? Again calculate plain text value from cipher text.

Solution:

1. Two prime numbers p = 3, q = 11
2. n = p * q = 3 * 11 = 33 **n = 33**
3. $\Phi(n) = (p-1) * (q-1) = (3 - 1) * (11 - 1) = 2 * 10 = 20$ **$\Phi(n) = 20$**
4. Public key e = 3. **e= 3**
5. Calculate d =7. $d = ((\Phi(n) * i) + 1) / e$ **d= 7**
6. Public key = {e, n} = {3, 33}, private key = {d, n} = {7, 33}.
7. Plain text $P = (00111011)_2 = (59)_{10}$, $C = P^e \bmod n = 59^3 \bmod 33 = 20$. **Cipher Text = 20**
8. Cipher text C = 20, $P = C^d \bmod n = 20^7 \bmod 33 = 26$. **Plain Text = 26**

Exercise - 5

Question: P and Q are two prime numbers. P=13, and Q=17. Take public key E=19. If original message is 12, then what will be cipher text value & private key value according to RSA algorithm? Again calculate plain text value from cipher text.

Solution:

1. Two prime numbers p = 13, q = 17
2. $n = p * q = 13 * 17 = 221$ **n = 221**
3. $\Phi(n) = (p-1) * (q-1) = (13 - 1) * (17 - 1) = 12 * 16 = 192$ **Φ(n) = 192**
4. Public key e = 19. **e= 19**
5. Calculate d =91. $d = ((\Phi(n) * i) + 1) / e$ **d= 91**
6. Public key = {e, n} = {19, 221}, private key = {d, n} = {91, 221}.
7. Plain text P = 12 , $C = P^e \bmod n = 12^{19} \bmod 221 = 181$. **Cipher Text = 181**
8. Cipher text C = 181, $P = C^d \bmod n = 181^{91} \bmod 221 = 12$. **Plain Text = 12**

Diffie-Hellman

The Diffie Hellman algorithm widely known as Key exchange algorithm or key agreement algorithm developed by Whitefield Diffie and Martin Hellman in 1976. The purpose of the algorithm is to enable two users to securely exchange a key that can be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of secret values.

Step-1: Select q (prime number) and α (α is primitive root of q)

Step-2: User A Key Generation: select X_A, $X_A < q$

Calculate **public key Y_A**, $Y_A = \alpha^{X}{}_A \bmod q$

Y_A Shared with user B

Step-3: User B Key Generation: select X_B, $X_B < q$

Calculate **public key Y_B**, $Y_B = \alpha^{X}{}_B \bmod q$

Y_B shared with user A

Step-4: Calculation of **secret key by user A**: $K = (Y_B)^{X}{}_A \bmod q$

Step-5: Calculation of **secret key by user B**: $K = (Y_A)^{X}{}_B \bmod q$

Diffie Helman Step by Step

Step – 1: Select q (prime number) and α (α is primitive root of q)

Example, here q = 7, α = 17.

Step – 2: User A Key Generation: Select $X_A < q$,

calculate **public key Y_A** and shared with user B: $Y_A = \alpha^{X}{}_{A} \bmod q$

Example, Here $X_A = 6$,

Calculate $Y_A = \alpha^{X}{}_{A} \bmod q \Rightarrow 17^6 \bmod 7 \Rightarrow 1$

Step – 3: User B Key Generation: Select $X_B < q$,

calculate **public key Y_B** and shared with user A: $Y_B = \alpha^{X}{}_{B} \bmod q$

Example, Here $X_B = 4$,

Calculate $Y_B = \alpha^{X}{}_{B} \bmod q \Rightarrow 17^4 \bmod 7 \Rightarrow 4$

Diffie Helman Step by Step- Cont

Step – 4: Calculation of **secret key by user A**:

$K = (Y_B)^{X_A} \bmod q$

Example, Here $Y_B = 4$, $X_A = 6$

Calculate $K = (Y_B)^{X_A} \bmod q \Rightarrow 4^6 \bmod 7 \Rightarrow 1$

Step – 5: Calculation of **secret key by user B**:

$K = (Y_A)^{X_B} \bmod q$

Example, Here $Y_A = 1$, $X_B = 4$

Calculate $K = (Y_A)^{X_B} \bmod q \Rightarrow 1^4 \bmod 7 \Rightarrow 1$

Exercise - 1

Exercise – 1: $q = 353$, $\alpha = 3$, $X_A = 97$, $X_B = 233$.

Determine ***Public Key*** and ***Shared key*** for both users using Diffie-Hellman key exchange algorithm.

Exercise - 1

Exercise – 1: $q = 353, \alpha = 3, X_A = 97, X_B = 233.$

Determine ***Public Key*** and ***Shared key*** for both users using Diffie-Hellman key exchange algorithm.

Solution:

1. Here $q = 353, \alpha = 3$
2. Calculate *Public key for user A*. $X_A = 97$,

   $Y_A = \alpha^{X_A} \bmod q = 3^{97} \bmod 353 = 40$ **$Y_A = 40$**
3. Calculate *Public key for user B*. $X_B = 233$,

   $Y_B = \alpha^{X_B} \bmod q = 3^{233} \bmod 353 = 248$ **$Y_B = 248$**
4. Calculation of *secret key by user A*,

   $K = (Y_B)^{X_A} \bmod q = 248^{97} \bmod 353 = 160$ **$K = 160$**
5. Calculation of *secret key by user B*,

   $K = (Y_A)^{X_B} \bmod q = 40^{233} \bmod 353 = 160$ **$K = 160$**

Exercise - 2

Exercise – 2: $q = 23, \alpha = 5, X_A = 6, X_B = 15.$

Determine ***Public Key*** and ***Shared key*** for both users using Diffie-Hellman key exchange algorithm.

Solution:

1. Here $q = 23, \alpha = 5$
2. Calculate *Public key for user A*. $X_A = 6,$

   $$Y_A = \alpha^{X_A} \bmod q = 5^6 \bmod 23 = 8$$

   $Y_A = 8$
3. Calculate *Public key for user B*. $X_B = 15,$

   $$Y_B = \alpha^{X_B} \bmod q = 5^{15} \bmod 23 = 19$$

   $Y_B = 19$
4. Calculation of *secret key by user A*,

   $$K = (Y_B)^{X_A} \bmod q = 19^6 \bmod 23 = 2$$

   $K = 2$
5. Calculation of *secret key by user B*,

   $$K = (Y_A)^{X_B} \bmod q = 8^{15} \bmod 23 = 2$$

   $K = 2$

Exercise - 3

Exercise – 3: $q = 11, \alpha = 17, X_A = 8, X_B = 12.$

Determine ***Public Key*** and ***Shared key*** for both users using Diffie-Hellman key exchange algorithm.

Solution:

1. Here $q = 11, \alpha = 17$
2. Calculate *Public key for user A*. $X_A = 8$,

   $Y_A = \alpha^{X_A} \bmod q = 17^8 \bmod 11 = 4$ **$Y_A = 4$**
3. Calculate *Public key for user B*. $X_B = 12$,

   $Y_B = \alpha^{X_B} \bmod q = 17^{12} \bmod 11 = 3$ **$Y_B = 3$**
4. Calculation of *secret key by user A*,

   $K = (Y_B)^{X_A} \bmod q = 3^8 \bmod 11 = 5$ **$K = 5$**
5. Calculation of *secret key by user B*,

   $K = (Y_A)^{X_B} \bmod q = 4^{12} \bmod 11 = 5$ **$K = 5$**

Cryptographic Protocols: Key Exchange

Cryptographic protocols are exchanges of messages carried out by two or more parties to achieve a particular security goal.

Key exchange is a protocol by which two parties can exchange a secret key over an **insecure channel** without having any past shared secret information. Here the *Diffe-Hellman key agreement protocol* is described by example.

1. Suppose that Alice and Bob want to share a common key.
2. Alice and Bob agree to use a prime p and a primitive root a of p.
3. Alice chooses a secret integer k_1 and sends a^{k1} **mod** p to Bob.
4. Bob chooses a secret integer k_2 and sends a^{k2} **mod** p to Alice.
5. Alice computes $(a^{k2})^{k1}$ **mod** p.
6. Bob computes $(a^{k1})^{k2}$ **mod** p.

At the end of the protocol, Alice and Bob have their shared key

$$(a^{k2})^{k1} \textbf{ mod } p = (a^{k1})^{k2} \textbf{ mod } p.$$

To find the secret information from the public information would require the adversary to find k_1 and k_2 from a^{k1} **mod** p and a^{k2} **mod** p respectively. This is an instance of the discrete logarithm problem, considered to be computationally infeasible when p and a are sufficiently large.

Cryptographic Protocols: Digital Signatures

Adding a *digital signature* to a message is a way of ensuring the recipient that the message came from the purported sender.

Suppose that Alice's RSA public key is (n,e) and her private key is d. Alice encrypts a plain text message x using $E_{(n,e)}(x) = x^d \bmod n$. She decrypts a ciphertext message y using $D_{(n,e)}(y) = y^d \bmod n$.

Alice wants to send a message M so that everyone who receives the message knows that it came from her.

1. She translates the message to numerical equivalents and splits into blocks m_1, m_2 , m_3,…. just as in RSA encryption.
2. She then applies her decryption function $D_{(n,e)}$ to the blocks and sends the results to all intended recipients.
3. The recipients apply Alice's encryption function and the result is the original plain text since $E_{(n,e)}(D_{(n,e)}(x)) = x$.

Everyone who receives the message can then be certain that it came from Alice.

Cryptographic Protocols: Digital Signatures

Example: Suppose Alice's RSA cryptosystem is the same as in the earlier example with key$(2537,13)$, $2537 = 43 \cdot 59$, $p = 43$ and $q = 59$ are primes and gcd(e,$(p-1)(q-1)$) = gcd$(13, 42 \cdot 58) = 1$.

Her decryption key is d = 937.

She wants to send the message "MEET AT NOON" to her friends so that they can be certain that the message is from her.

Solution: Alice translates the message into blocks of digits $1204\ 0419\ 0019\ 1314\ 1413$.

1. She then applies her decryption transformation $D_{(2537,13)}$ (x)= x^{937} **mod** 2537 to each block.
2. She finds (using her laptop, programming skills, and knowledge of discrete mathematics) that 1204^{937} **mod** $2537 = 817$, 419^{937} **mod** $2537 = 555$, 19^{937} **mod** $2537 = 1310$, 1314^{937} **mod** $2537 = 2173$, and 1413^{937} **mod** $2537 = 1026$.
3. She sends $0817\ 0555\ 1310\ 2173\ 1026$.

When one of her friends receive the message, they apply Alice's encryption transformation $E_{(2537,13)}$ to each block. They then obtain the original message which they translate back to English letters.