Discrete Mathematics
Lecture 3

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

Summary of Lecture 2

Sum of ideals: $a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\mathbb{Z}$. $\{a,b\} \neq \{0\}$

Greatest common divisor: $\gcd(a,b) = as + bt$.

- $c|ab, \gcd(c,a) = 1 \Rightarrow c|b$
- p is a prime, $p|ab \Rightarrow p|a$ or $p|b$
- Uniqueness proof for FTA
- Infinity of primes

Equivalence relation: a binary relation R on a set A

- reflexive, symmetric, transitive
- equivalence class $[a]_R$

Congruence: $R = \{(a,b) \in \mathbb{Z}^2 : n|(a-b)\}$

- $a \equiv b \pmod{n}$: $(a,b) \in R$
- $a = bq + r$: $a \bmod n = r$
- $[a]_n$

Residue Class

DEFINITION: Let $\alpha \in \mathbb{R}$.

- $\lfloor \alpha \rfloor$: **floor** of α, the largest integer $\leq \alpha$
- $\lceil \alpha \rceil$: **ceiling** of α, the smallest integer $\geq \alpha$
  - If $a = bq + r$, then $q = \lfloor a/b \rfloor$ and $r = a - bq$

DEFINITION: Let $a \in \mathbb{Z}, n \in \mathbb{Z}^+$. We denote the equivalence class of a under the equivalence relation mod n with $[a]_n$ and call it the **residue class of** a mod n.

- $[a]_n = a + n\mathbb{Z} = \{a + nx : x \in \mathbb{Z}\}$ 代表元
  - any element of $[a]_n$ is a **representative** of $[a]_n$

EXAMPLE: $[0]_6 = \{0, \pm 6, \pm 12, \ldots\}$; $[1]_6 = \{\ldots, -11, -5, 1, 7, 13, \ldots\}$; ...

Residue Class

THEOREM: Let $n \in \mathbb{Z}^+, a, b \in \mathbb{Z}$. Then

$$[a]_n \cap [b]_n = \emptyset \text{ or } [a]_n = [b]_n.$$

- $[a]_n \cap [b]_n = \emptyset$: done
- $[a]_n \cap [b]_n \neq \emptyset$
  - $\exists c \in [a]_n \cap [b]_n$
  - $c \equiv a \pmod{n}, c \equiv b \pmod{n}$
  - $a \equiv b \pmod{n}$
  - $\exists t \in \mathbb{Z}$ such that $a = b + nt$
  - $[a]_n = \{a + nx: x \in \mathbb{Z}\} = \{b + nt + nx: x \in \mathbb{Z}\} = [b]_n$

推论

COROLLARY: $[a]_n = [b]_n$ iff $a \equiv b \pmod{n}$.

Z的划分

COROLLARY: $\{[0]_n, [1]_n, \dots, [n-1]_n\}$ is a partition of $\mathbb{Z}$.

- $[a]_n \cap [b]_n = \emptyset$ for all $a, b \in \{0,1, \dots, n-1\}$
- $\mathbb{Z} = [0]_n \cup [1]_n \cup \cdots \cup [n-1]_n$

$\mathbb{Z}_n$

DEFINITION: Let n be any positive integer. We define $\mathbb{Z}_n$ to be set of all residue classes modulo n.

- $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$
  - $\mathbb{Z}_n = \{0,1,\ldots,n-1\}$;

表示不唯一

任选代表元

- $\mathbb{Z}_n = \{[1]_n, [2]_n, \ldots, [n]_n\}$
  - $\mathbb{Z}_n = \{1,2,\ldots,n\}$

EXAMPLE: Two representations of the set $\mathbb{Z}_6$

- $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$
  $= \{0,1,2,3,4,5\}$
- $\mathbb{Z}_6 = \{[-3]_6, [-2]_6, [-1]_6, [0]_6, [1]_6, [2]_6\}$
  $= \{-3,-2,-1,0,1,2\}$

$\mathbb{Z}_n$

DEFINITION: Let $n \in \mathbb{Z}^+$. For all $[a]_n, [b]_n \in \mathbb{Z}_n$, define

- **addition**: $[a]_n + [b]_n = [a+b]_n$
- **subtraction**: $[a]_n - [b]_n = [a-b]_n$
- **multiplication**: $[a]_n \cdot [b]_n = [a \cdot b]_n$

Well-defined? If $a \equiv a' \pmod n$ and $b \equiv b' \pmod n$, then

$a \pm b \equiv a' \pm b' \pmod n$ and $ab \equiv a'b' \pmod n$.

- Hence, $[a]_n \pm [b]_n = [a']_n \pm [b']_n$; $[a]_n \cdot [b]_n = [a']_n \cdot [b']_n$
    - $a \equiv a' \pmod n \Rightarrow n | (a - a') \Rightarrow \exists x$ such that $a - a' = nx$
    - $b \equiv b' \pmod n \Rightarrow n | (b - b') \Rightarrow \exists y$ such that $b - b' = ny$
        - $(a+b) - (a'+b') = nx + ny$
        - $(a-b) - (a'-b') = nx - ny$
        - $ab - a'b' = a(b - b') + b'(a - a') = any + b'nx$

$\mathbb{Z}_n^*$

DEFINITION: Let $n \in \mathbb{Z}^+$ and $[a]_n \in \mathbb{Z}_n$. $[s]_n \in \mathbb{Z}_n$ is called an **inverse** of $[a]_n$ if $[a]_n[s]_n = [1]_n$.

- **division**: If $[a]_n\ [s]_n = [1]_n$, define $\frac{[b]_n}{[a]_n} = [b]_n \cdot [s]_n$

THEOREM: Let $n \in \mathbb{Z}^+$. $[a]_n \in \mathbb{Z}_n$ has an inverse iff $\gcd(a, n) = 1$.

- Only if: $\exists\ s$ s.t. $[a]_n[s]_n \equiv [1]_n$; $\exists\ t, as - 1 = nt$; $\gcd(a, n) = 1$
- If: $\exists\ s, t$ s.t. $as + nt = 1$; $as \equiv 1 \pmod{n}$

DEFINITION: Let $n \in \mathbb{Z}^+$. Define $\mathbb{Z}_n^* = \{[a]_n \in \mathbb{Z}_n\colon \gcd(a, n) = 1\}$

- If n is prime, then $\mathbb{Z}_n^* = \{1,2, \dots, n-1\}$
- If n is composite, then $\mathbb{Z}_n^* \subset \mathbb{Z}_n$

EXAMPLE: $\mathbb{Z}_5^* = \{1,2,3,4\}$; $\mathbb{Z}_6^* = \{1,5\}$; $\mathbb{Z}_8^* = \{1,3,5,7\}$

Euler's Phi Function

QUESTION: How many elements are there in $\mathbb{Z}_n^*$?

- $|\mathbb{Z}_n^*|$ is the number of integers $a \in [n]$ such that $\gcd(a, n) = 1$

DEFINITION: (Euler's Phi Function) $\phi(n) = |\mathbb{Z}_n^*|, \forall n \in \mathbb{Z}^+$.

- $\phi(n)$ is the number of integers $a \in [n]$ such that $\gcd(a, n) = 1$

THEOREM: Let p be a prime. Then $\forall e \in \mathbb{Z}^+, \phi(p^e) = p^{e-1}(p-1)$.

- Let $x \in [p^e]$.
- $\gcd(x, p^e) \neq 1$ iff $p|x$
  iff $x = p, 2p, \ldots, p^{e-1} \cdot p$
  - $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$

EXAMPLE: $\phi(3^2) = 3(3-1) = 6$

- $\mathbb{Z}_9^* = \{1,2,\cancel{3},4,5,\cancel{6},7,8,\cancel{9}\}$

EXAMPLE: $\phi(p) = p - 1$

- $\mathbb{Z}_p^* = \{1,2, \ldots, p-1\}$

Euler's Phi Function

先算 $n-\varphi(n)$

QUESTION: Formula of $\phi(n)$ for general integer n?

THEOREM: If $n = p_1^{e_1} \cdots p_k^{e_k}$ for distinct primes $p_1, \ldots, p_k$ and integers $e_1, \ldots, e_k \geq 1$, then $\boxed{\phi(n) = \phi(p_1^{e_1}) \cdots \phi(p_k^{e_k}).}$ 目前先不证

Hence, $\phi(n) = n(1 - p_1^{-1}) \cdots (1 - p_k^{-1})$.

- There are many proofs. We will see in the future.

COROLLARY: If $n = pq$ for two different primes p and q, then $\phi(n) = (p-1)(q-1)$.

EXAMPLE: $\phi(10) = (2-1)(5-1) = 4; n = 10; p = 2, q = 5$

- $\mathbb{Z}_{10}^* = \{1, \cancel{2}, 3, \cancel{4}, \cancel{5}, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}\}$

Euler's Theorem

THEOREM (Euler) Let $n \geq 1$ and $\alpha \in \mathbb{Z}_n^*$. Then $\alpha^{\phi(n)} \equiv 1$. mod n

- $\alpha^{\phi(n)}, 1$ are both residue classes modulo n
- Suppose that $\alpha = [a]_n$ for $a \in \mathbb{Z}$. Then $\alpha^{\phi(n)} = 1$ is $([a]_n)^{\phi(n)} = [1]_n$
- How to prove?
  - Consider the map $f\colon \mathbb{Z}_n^* \to \mathbb{Z}_n^* \quad [x]_n \mapsto [a]_n \cdot [x]_n$
  - We show that f is injective 单射
    - $f([x]_n) = f([y]_n)$
    - $[a]_n \cdot [x]_n = [a]_n \cdot [y]_n$
    - $[ax]_n = [ay]_n$
    - $n | a(x - y)$
    - $n | (x - y)$, this is because $\gcd(n, a) = 1$
      - $[x]_n = [y]_n$

元素个数相同

Euler's Theorem

THEOREM (Euler) Let $n \geq 1$ and $\alpha \in \mathbb{Z}_n^*$. Then $\alpha^{\phi(n)} = 1$.

- $\alpha^{\phi(n)}, 1$ are both residue classes modulo n
- Suppose that $\alpha = [a]_n$ for $a \in \mathbb{Z}$. Then $\alpha^{\phi(n)} = 1$ is $([a]_n)^{\phi(n)} = [1]_n$
- How to prove?
  - Consider the map $f\colon \mathbb{Z}_n^* \to \mathbb{Z}_n^* \quad [x]_n \mapsto [a]_n \cdot [x]_n$
  - Suppose that $\mathbb{Z}_n^* = \left\{[x_1]_n, \ldots, \left[x_{\phi(n)}\right]_n\right\}$.
    - $f([x_1]_n) \cdots f\left(\left[x_{\phi(n)}\right]_n\right) = [x_1]_n \cdots \left[x_{\phi(n)}\right]_n$
    - $[ax_1]_n \cdots \left[ax_{\phi(n)}\right]_n = [x_1]_n \cdots \left[x_{\phi(n)}\right]_n$
    - $\left[a^{\phi(n)}x_1 \cdots x_{\phi(n)}\right]_n = \left[x_1 \cdots x_{\phi(n)}\right]_n$
      - $n | \left(a^{\phi(n)} - 1\right)x_1 \cdots x_{\phi(n)}$
        - $n | \left(a^{\phi(n)} - 1\right)$, this is because $\gcd\left(n, x_1 \cdots x_{\phi(n)}\right) = 1$
          - $\left[a^{\phi(n)}\right]_n = [1]_n$, i. e., $([a]_n)^{\phi(n)} = [1]_n$

Fermat's Little Theorem

EXAMPLE: Understand Euler's theorem with $\mathbb{Z}_{10}^* = \{1,3,7,9\}$.

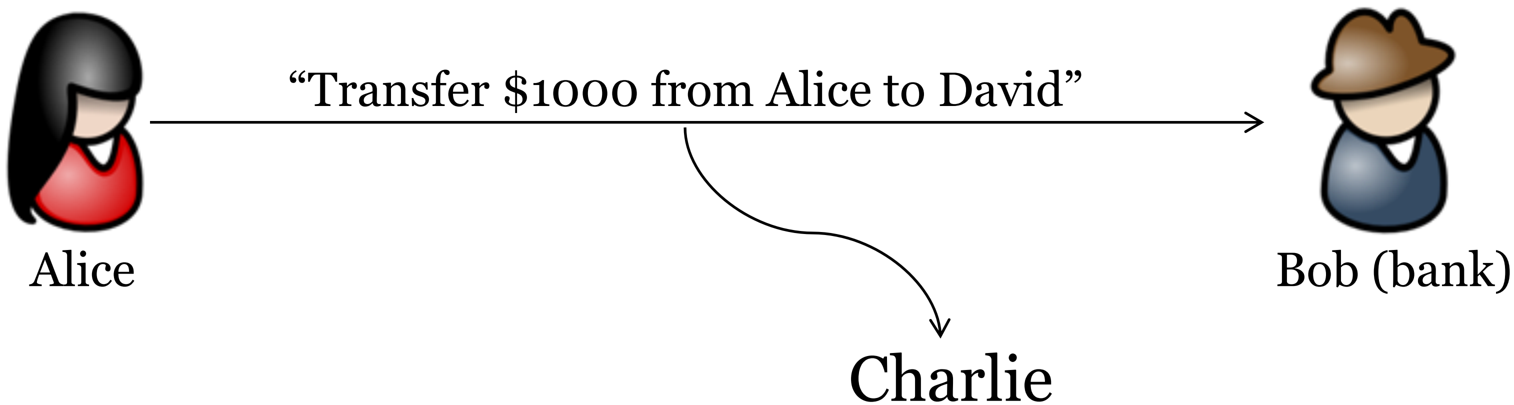
- $n = 10, \phi(n) = 4,$
- $1^4 \equiv 1 \pmod{10} \Rightarrow ([1]_{10})^4 = [1]_{10}$
- $3^4 = 81 \equiv 1 \pmod{10} \Rightarrow ([3]_{10})^4 = [1]_{10}$
- $7^4 = 2401 \equiv 1 \pmod{10} \Rightarrow ([7]_{10})^4 = [1]_{10}$
- $9^4 = 6561 \equiv 1 \pmod{10} \Rightarrow ([9]_{10})^4 = [1]_{10}$
    - Consider the map $f\colon \mathbb{Z}_{10}^* \to \mathbb{Z}_{10}^* \quad [x]_n \mapsto [9]_n \cdot [x]_n$
    - $f([1]_{10}) = [9]_{10} \cdot [1]_{10} = [9]_{10}; f([3]_{10}) = [7]_{10}; f([7]_{10}) = [3]_{10}, f([9]_{10}) = [1]_{10}$
    - f is injective
    - $f([1]_{10})f([3]_{10})f([7]_{10})f([9]_{10}) = [9]_{10}[7]_{10}[3]_{10}[1]_{10}$

Fermat's Little Theorem: If p is a prime and $\alpha \in \mathbb{Z}_p$.

Then $\alpha^p = \alpha$.

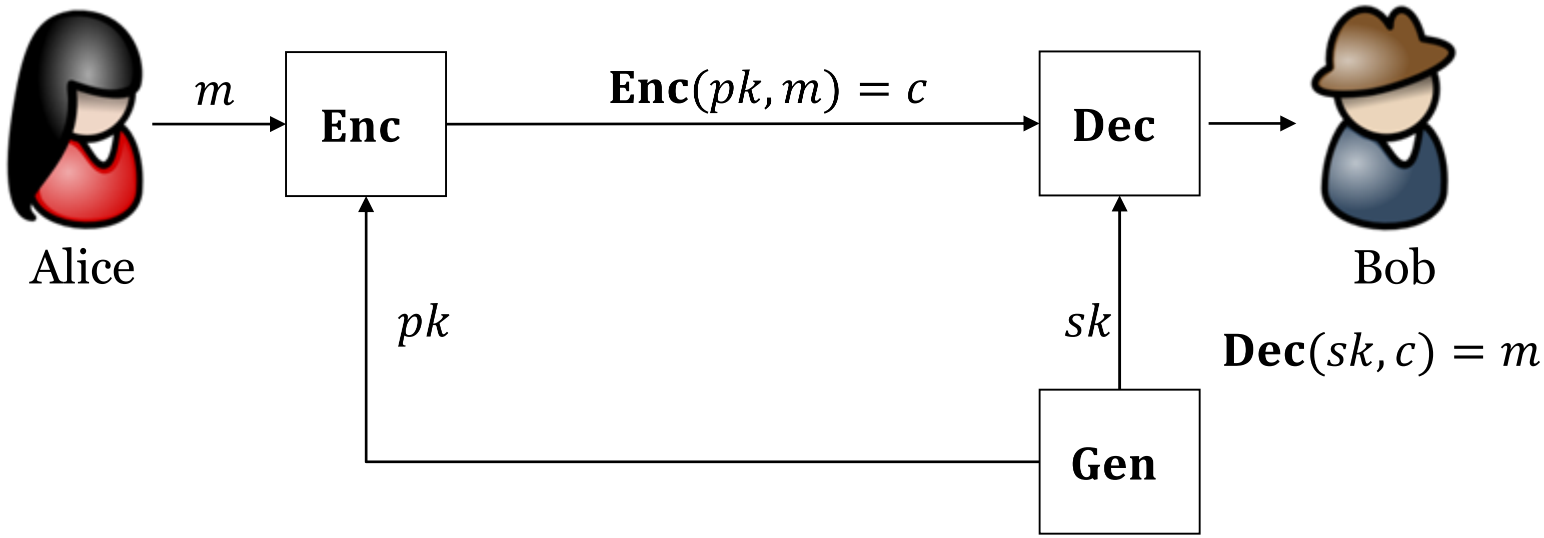
- This is a corollary of Euler's theorem for $n = p$
- By Euler's theorem, $\alpha^{p-1} = 1$
    - $\alpha^p = \alpha$

Cryptography



- **Confidentiality**: The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes. --FIPS 140-2

Public-Key Encryption

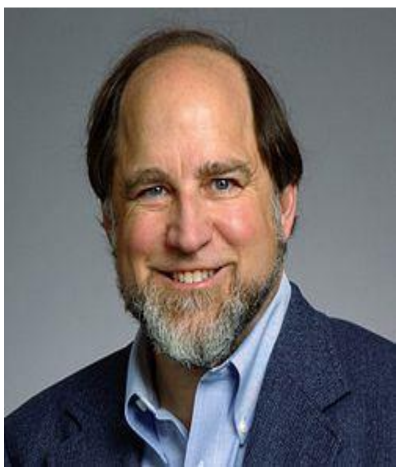


- **Gen**, **Enc**, **Dec**: key generation, encryption, decryption
- m, c, pk, sk: plaintext (message), ciphertext, public key, private key
- $\mathcal{M}, \mathcal{C}$: plaintext space, ciphertext space
  - $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}) + \mathcal{M}, |\mathcal{M}| > 1$
    - **Correctness**: $\mathbf{Dec}\big(sk, \mathbf{Enc}(pk, m)\big) = m$ for any pk, sk, m
    - **Security**: if sk is not known, it's difficult to learn m from pk, c

RSA

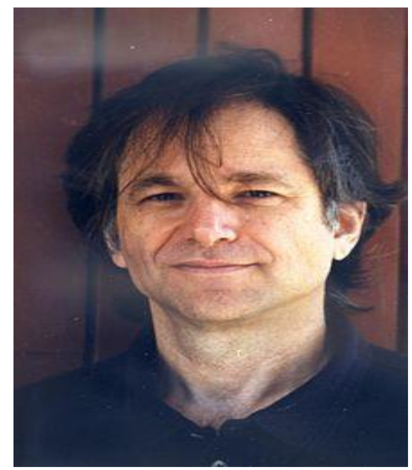
A method for obtaining digital signatures and public-key cryptosystem

- Ronald Rivest, Adi Shamir and Leonard Adleman (1977)-MIT
- Scientific Contributions: Turing Award (2002)
  - Public-Key Encryption: the first construction
  - Digital Signature: the first construction



Rivest

Shamir



Adleman

Plain RSA

CONSTRUCTION: $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}) + \mathcal{M}$, the message space is $\mathcal{M} = \{m: m \in [N], \gcd(m, N) = 1\}$

- $(pk, sk) \leftarrow \mathbf{Gen}(1^n)$
  - choose two n-bit primes $p \neq q$;
  - $N = pq$; $\phi(N) = (p-1)(q-1)$
  - $[e]_{\phi(N)} \leftarrow \mathbb{Z}^*_{\phi(N)}$
  - $[d]_{\phi(N)} = \left([e]_{\phi(N)}\right)^{-1}$
    - $0 \leq e, d < \phi(N)$ $e = 0?$
  - output $pk = (N, e)$ and $sk = (N, d)$
- $c \leftarrow \mathbf{Enc}(pk, m)$:
  - output $c = m^e \bmod N$
    - $0 \leq c < N$
- $m \leftarrow \mathbf{Dec}(sk, c)$:
  - output $m = c^d \bmod N$
    - $0 \leq m < N$

?Dec$(sk, \mathbf{Enc}(pk, m)) = m$

- $[d]_{\phi(N)} = \left([e]_{\phi(N)}\right)^{-1}$
- $\exists t \in \mathbb{Z}$ s.t. $ed = 1 + t \cdot \phi(N)$
- $[c^d]_N = ([c]_N)^d$
  $= ([m^e]_N)^d$
  $= \left(([m]_N)^e\right)^d$
  $= ([m]_N)^{ed}$
  $= ([m]_N)^{1+t\phi(N)}$
  $= [m]_N \cdot ([m]_N)^{\phi(N)t}$
  $= [m]_N \cdot [1]_N$
  $= [m]_N$
- $m = c^d \bmod N$

RSA is correct!

Plain RSA

EXAMPLE: this is a toy example; all numbers are very small

- $(pk, sk) \leftarrow \mathbf{Gen}(1^n)$
  - $p = 7, q = 13,$
  - $N = 91, \phi(N) = 72$
  - $[e]_{72} = [5]_{72}$
  - $[d]_{72} = [29]_{72}$
  - $pk = (91, 5);\ sk = (91, 29)$
- $c \leftarrow \mathbf{Enc}(pk, m)$: $m = 2$
  - $c = (2^5 \bmod 91) = 32$
- $m \leftarrow \mathbf{Dec}(sk, c)$: $c = 10$
  - $m = (32^{29} \bmod 91) = 2$

- $32^{29} = (2^5)^{29} = 2^{145}$
- $2^{145} \equiv ?\ (\mathrm{mod}\ 91)$
- $[2^{145}]_{91} = [?\,]_{91}$
- $([2]_{91})^{145} = [?\,]_{91}$
- $[2]_{91} \in \mathbb{Z}_{91}^*$
- $([2]_{91})^{\phi(91)} = [1]_{91}$
- $$\begin{aligned}([2]_{91})^{145} &= ([2]_{91})^{72}([2]_{91})^{72}[2]_{91} \\ &= [1]_{91}[1]_{91}[2]_{91} \\ &= [2]_{91}\end{aligned}$$

Security

Security: If sk is not known, it's difficult to learn m from pk, c

- At least, it should be difficult to learn d from pk

Plain RSA and Integer Factoring (given N, find p, q**):**

- "Factoring is easy" ⇒ "Plain RSA is not secure"
  - $N \rightarrow (p, q) \rightarrow \phi(N) \rightarrow d$: computable with EEA
- "Plain RSA is secure" ⇒ "Factoring is hard"
- "Factoring is hard"⇏ "Plain RSA is secure"
- It is likely that "Factoring is hard"⇒ "Plain RSA is secure"
  - The best known method of computing d is via factoring N

How Large is the N in practice?

- $|N| = 2048$ is recommended from present to 2030
- $|N| = 3072$ is recommended after 2030

RSA

EXAMPLE: A sample execution of the RSA public-key encryption.

- p =179769313486231590772930519078902473361797697894230657273430081157732675805500963132708477322407536021120113879871393357658789768814416622492847430639474124377767893424865485276302219601246094119453082952085005768838150682342462881473913110540827237163350510684586298239947245938479716304835356329624225795083
- q =179769313486231590772930519078902473361797697894230657273430081157732675805500963132708477322407536021120113879871393357658789768814416622492847430639474124377767893424865485276302219601246094119453082952085005768838150682342462881473913110540827237163350510684586298239947245938479716304835356329624227077847
- N =323170060713110073007148766886699519604441026697154840321303454275246551388678908931972014115229134636887179609218980194941195591504909210950881523864482831206308773673009960917501977503896521067960576383840675682767922186426197561618380943384761704705816458520363050428875758915410658086075523991239312121907428611986660485601310980814305187748463472592153326117591493307252524372764241478178087292737551655273799645610742645870326647095113460183277983737152901481295041417951323149293889926882474402327275395755146886332824477192285306647065209393578785285402841841565134055758720857034205009699669179513813108263 01
- $\phi(N)$ =323170060713110073007148766886699519604441026697154840321303454275246551388678908931972014115229134636887179609218980194941195591504909210950881523864482831206308773673009960917501977503896521067960576383840675682767922186426197561618380943384761704705816458520363050428875758915410658086075523991239312121903833225716935853785852370432727138281227518634268712972122891684097870856654222215523917746289400934851397368013314778717150851718825127733421035124363418993739683549454013443767845534857552519938213736713446770956061463545436049017586947182762240542135831627873408090959775938264610683602962052921328579533 72

RSA

EXAMPLE: A sample execution of the RSA public-key encryption.

- e =15
- d =4308934142841467640095316891822660261392547022628731204284046057003287351849052119092960
  1882030551284918290614562530692658826078867321228126784203181931044160841169823067994789000
  2636671862028090614101845120900910357229581901596748824507924513015606274421944693817400571
  8343452205475441147673653216524161625384443009559144717144698272436361843749700248456916172
  9616385557879716114220562962069855699505253457980186315735108637162286780229176683697789471
  3499151225324986244732605351258357127379810070026584284982284595694608081951393914732023449
  26291034965405618110883716454412127970125101948091147061607056177143937 83
- m =1060492175475872144576165469414485300895277760828043761504547236562152874067991556927005
  1503191522500036448557172487959011926112038398359402756573149541644330968641767630622070720
  6300611302597838253559482233713309491580368127421870570456049345468117909489758782001441890
  4834424987320032029927723446568903940998962231923268398424184371118321200199145779352875281
  2978134072787404790207031482099444968252108690296363773578594703102617386738297675080295774
  0914472401975212215460354590300865381144285160786447331806555401091337782416072602736553356
  61777894173665137928787960365220712025120785257907244561721692764755210375
- c =1052638995813896291959559409341115889309974350846590234712847813990877461431177809735479
  5345791726768384252751637693995592403757856185437083738829836072472243389583367910268799453
  3780394197213455665495167301873084368644600883966117266700507232420801391760803347202941953
  0404891500380565634181654830724988604902791048824931866006271433570305757657601698851348414
  8308512574950252535463185824865665499749033598201370342142901944632549253564037639312442875
  0397358269093293568406659937836951014476104859227269159699679685846612404304259821941895044
  004698897625742758242694754953949201079210667232777692261994755580686270 49

Questions from RSA

CONSTRUCTION: $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}) + \mathcal{M}$, the message space is $\mathcal{M} = \{m: m \in [N], \gcd(m, N) = 1\}$

- $(pk, sk) \leftarrow \mathbf{Gen}(1^n)$
  - choose two n-bit primes $p \neq q$
  - $N = pq$; $\phi(N) = (p-1)(q-1)$
  - $[e]_{\phi(N)} \leftarrow \mathbb{Z}^*_{\phi(N)}$
  - $[d]_{\phi(N)} = \left([e]_{\phi(N)}\right)^{-1}$
    - $0 \leq e, d < \phi(N)$
  - output $pk = (N, e)$ and $sk = (N, d)$
- $c \leftarrow \mathbf{Enc}(pk, m)$:
  - output $c = m^e \bmod N$
    - $0 \leq c < N$
- $m \leftarrow \mathbf{Dec}(sk, c)$:
  - output $m = c^d \bmod N$
    - $0 \leq m < N$

How to choose p, q EFFICIENTLY?

How to compute d EFFICIENTLY?

How to compute c EFFICIENTLY?

How to compute m EFFICIENTLY?