Mathematics behind encryption of information

RSA, ASCII ..

primes

Number theory (Prime numbers)

Whole numbers, Integer numbers

$\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$ - set of integers

Def: $a, b \in \mathbb{Z}$ $a \mid b$ 'a divides b' if

$\exists\, c \in \mathbb{Z}$ s.t.

there exists $a \cdot c = b$ 'a is a divisor of b'

Ex: $6 \mid 18$ $6 \cdot 3 = 18$

$10 \mid 10$ $10 \cdot 1 = 10$

$7 \mid 0$ $7 \cdot 0 = 0$

$3 \nmid 5$ ← does not divide

Properties of divisibility

- if $a \mid b$, $b \mid c \Rightarrow a \mid c$

Proof: $a \cdot d = b$ ($d \in \mathbb{Z}$) $b \cdot f = c$ ($f \in \mathbb{Z}$) $c = b \cdot f = a \cdot (d \cdot f)$ ($d \cdot f \in \mathbb{Z}$)

- $a \mid b \Rightarrow a^{100} \mid b^{100}$ $\left(n \in \mathbb{Z}_+ = \{1, 2, 3, 4, \dots\} \text{ positive integers} \right)$

$a \cdot d = b$ ($d \in \mathbb{Z}$) $(a \cdot d)^{100} = b^{100}$

$a^{100} \cdot d^{100}$ ($d^{100} \in \mathbb{Z}$)

- if $a \mid x$, $a \mid y \Rightarrow a \mid m \cdot x + n y$ $\forall\, m, n \in \mathbb{Z}$

Proof: $\exists\, c, d \in \mathbb{Z}$ s.t.

$a \cdot c = x$, $a \cdot d = y$

$m x + n y = m \cdot a \cdot c + n \cdot a \cdot d = a(mc + nd)$ ($mc + nd \in \mathbb{Z}$)

Ex: $6 \mid 36$, $6 \mid 12$ $\Rightarrow$ $6 \mid 96$

$96 = 1 \cdot 36 + 5 \cdot 12$

Def: An even number x is $2 \mid x$

An odd number x is $2 \nmid x$

Theorem (Division algorithm)

Let $a, b \in \mathbb{Z}$, $b > 0$. Then $\exists$ unique $q, r \in \mathbb{Z}$ s.t. $a = b \cdot q + r$, $0 \le r < b$

Ex: $a = 100$, $b = 3$

$100 = 3 \cdot q + r$ (r remainder, q quotient)

$q = 33$, $r = 1$

Idea: increase q until $100 - 3 \cdot q$ becomes negative $\Rightarrow$ too far

Proof: First, find q, r, then prove uniqueness

Let $S = \{ a + by \mid y \in \mathbb{Z} \}$

$S^+ \subset S$ – subset of nonnegative numbers in S

Let r – the smallest element in S^+

$a = 100$, $b = 3$

$S = \{ \dots -5, -2, 1, 4, 7, 10, \dots, 100, 103, 106 \dots \}$

$y = -36$, $y = 0$

$S^+ = \{ 1, 4, 7, 10, \dots \}$

r

Claim: $0 \le r < b$ since $r \in S$ $r = a + by$ for some y

$r \ge 0$ since $r \in S^+$

Suppose $r \ge b$: $r' = r - b = a + by - b = a + b(y-1) > 0$, $y - 1 \in \mathbb{Z}$

$\Rightarrow r' \in S^+$

Contradiction, since r is the smallest element in S^+

$\Rightarrow r < b$

$r = a + by \Rightarrow a = r + b(-y)$, $q = -y$

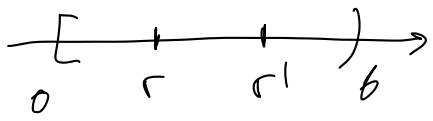
Now let us prove uniqueness

$\exists\ r, q;\ r', q' \in \mathbb{Z}$ s.t.

$$\begin{cases} a = bq + r, & 0 \le r < b \\ a = bq' + r', & 0 \le r' < b \end{cases} \qquad r, r' \in [0, b)$$

$0 = a - a = bq + r - bq' - r' = b(q - q') + (r - r')$

$b(q-q') = r'-r \quad \Rightarrow \quad b \mid r'-r$



$\Downarrow$

$|r'-r| < b$

$r'-r = 0$

$r' = r$

$b(q-q') = 0, \quad b > 0$

$q = q'$

Ex: Show that $5 \mid n^5 - n \quad \forall n \in \mathbb{Z}_+$

base: $n=1$ ✓ $5 \mid 1^5 - 1 \quad 5 \mid 0$ true

$n=2$ $2^5 - 2 = 32 - 2 = 30 \quad 5 \mid 30$

$5 \mid 3^5 - 3$

If $5 \mid n^5 - n \Rightarrow$

$n^5 - n \equiv 0 \pmod 5$

Mathematical induction

assumption: Assume $\exists k \in \mathbb{Z}_+$ s.t. $5 \mid k^5 - k$

Induction step: $5 \mid (k+1)^5 - (k+1)$

$$(k+1)^5 - (k+1) = k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1 - k - 1$$

$$= \underbrace{k^5 - k}_{5 \mid k^5 - k} + \underbrace{5(k^4 + 2k^3 + 2k^2 + k)}_{\in \mathbb{Z}}$$

divisible by 5

By induction $5 \mid n^5 - n \quad \forall n \in \mathbb{Z}_+$

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
$n=5 \rightarrow$ 1 5 10 10 5 1

$\ell \in \mathbb{Z}$

$n^5 - n = 5 \cdot \ell$

$n=4$ ✓

$5 = 4+1$

$(4+1)^5 - (4+1)$

$4^5 - 4 = 5 \cdot p$

Primes: **Def** A number $p \in \mathbb{Z}$ is **prime** if $p > 0$ and has **exactly two divisors**: p and 1. Otherwise the number is called composite

$p = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$, $\ell \in \mathbb{Z}$, $k_1 \dots k_\ell \in \mathbb{Z}_+$

✗ 2, 3, 5, 7, 11, 13, 17, 19, 23 ----

94 049

1299 709 ---

The largest known prime: $2^{74,207,281} - 1 \sim 10^{21\,000\,000}$

$2^{50} \sim 10^{15}$ $\quad \log_{10} 2 = \frac{\log 2}{\log 10} \simeq 0.301$

$\pi(x) = \#$ primes $< x$

$\pi(10) = 4$

$\pi(20) = 8$

$\pi(100) = 25$ ←

$\pi(x) \approx \frac{x}{\log x}, \quad x \to \infty$

$\frac{100}{\log 100} \approx \frac{100}{4.6} \approx 22$

Finding primes (Sieve of Eratosthenes)

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~

$\sqrt{N}$

- cross out all multiples of 2 except 2
- circle the first non-crossed number
- do over

Need to iterate roughly $\sqrt{N}$ times

Why: If $a > \sqrt{N}$ $\quad a = 6, 7, 8 \ldots$

$K < N$ $\quad a \mid K$ is K already crossed out?

$a \mid K \Rightarrow K = a \cdot c, \ c \in \mathbb{Z}$ $\quad c \mid K$

$K < N, \ a > \sqrt{N} \Rightarrow c < \sqrt{N}$

then K is a multiple of c and it had been crossed out.

Fun HW: Write a code which calculates the largest prime possible on your machine.

Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37

1 2 2 4 2 4 2 4 6 2 6 ← congruent to 1

$4k+1$: 5, 13, 17, 29 $\quad \equiv 1 \pmod 4$

$4k+3$: 3, 7, 11, 19, 23 .. $\quad \equiv 3 \pmod 4$

Theorem: There are infinitely many primes.

Idea: $a \mid b, \ a > 1 \Rightarrow a \nmid b+1$

$6 \mid 12$ $\quad 6 \nmid 13$

$7 \mid 21$ $\quad 7 \nmid 22$

$\exists \ c \in \mathbb{Z}$ s.t. $b = a \cdot c$

assume $a \mid b+1 \Rightarrow \exists \ d \in \mathbb{Z}$ s.t. $b+1 = a \cdot d$

$1 = (b+1) - b = a \cdot d - a \cdot c = a(d-c)$ ← $\mathbb{Z}$

$\Rightarrow a \mid 1$ impossible unless $a = 1$.

Proof of the theorem: Assume there are finitely many primes

$\mathcal{P} = \{p_1, p_2, \ldots, p_k\}$ – complete list of all primes

consider $N = p_1 \cdot p_2 \cdot \ldots \cdot p_k$, look at $N+1$

by construction $p_1 \mid N$, $p_2 \mid N$, …, $p_k \mid N$

but $p_1 \nmid N+1$, $p_2 \nmid N+1$, …, $p_k \nmid N+1$

Does $N+1$ have any divisors? Yes 1, $N+1$ if there are no others

then $N+1$ is prime

if there are: $N+1 = a \cdot b$, $a, b < N+1$

$a \mid N+1$.

Is a prime? Yes, no: $a = c \cdot d$

$c, d < a$

is c prime? Yes, no: $c = e \cdot f$

⋮ ⋮

this process will terminate when we find a prime

$p \mid N+1$

but $p \notin \mathcal{P}$ $\Rightarrow$ $\mathcal{P}$ does not contain all primes

Proposition: Given any $N \in \mathbb{Z}_+$ there are two consecutive primes which are $\geq N$ apart.

$p-1, p, p+1, \ldots, p'-1, p', p'+1$ $\quad p' - p \geq N$

$\geq N$

$(n+1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n \cdot (n+1)$ ← $(i+1)$

Proof: $n = N-1$: $a_i = (n+1)! + i+1$, $i = 1 \ldots n$

$n = N-1 \Leftarrow$ of composite numbers

$\begin{cases} a_1 = (n+1)! + 2 \\ a_2 = (n+1)! + 3 \\ \vdots \\ a_n = (n+1)! + (n+1) \end{cases}$

$n = 10$

$a_1 = 11! + 2 = 481,466,702$

$a_2 = 11! + 3 = 481,466,703$

$\vdots$

$a_{10} = 481,466,711$

$(i+1) \mid a_i \quad \forall \quad 1 \leq i \leq n$

≥ 2

$a_i = (i+1)\left(\frac{(n+1)!}{i+1} + 1\right)$ all a_i's are composite (not prime)

Next time: Modular arithmetic, Little Fermat theorem, Euler's theorem RSA encryption

The fundamental theorem of Arithmetic ($\mathbb{Z}$)

For every $N > 1$ $\exists$ a prime factorization of N:

$\exists$ distinct primes $p_1, p_2, \dots p_k$, $r_1 \dots r_k$, $r_i \geq 1$, $i = 1, \dots k$

s.t.

$$N = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$$

The factorization is unique up to reordering of the factors.

Ex: Complex numbers $a + \sqrt{-5}\,b$ $(\sqrt{-5})^2 = -5$

(Gaussian primes) $\mathbb{Z} \subset \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

- $(1+\sqrt{-5})(1-\sqrt{-5}) = 1 \cdot 1 - \sqrt{-5} \cdot \sqrt{-5} = 6$
- $2 \cdot 3 = 6$

Def: $a, b \in \mathbb{Z}$, not both zero. The greatest common divisor of a and b

$$\gcd(a,b) = (a,b) = d \in \mathbb{Z}$$

is the largest integer dividing a and b

Ex: $\gcd(100, 76) = 4$

$\gcd(6, 15) = 3$

$\gcd(150, 0) = 150$ $\quad 150 \mid 0$

$\gcd(20212021, 202120212021)$ $\quad 20212021 = 2021 \cdot 10001 + 0$

$202120212021 = 20212021 \cdot 10000 + 2021$

$\gcd \to 2021$

Euclidean Algorithm

Lemma: Let $a, b \in \mathbb{Z}$, $a, b \neq 0$

Then $\gcd(a,b) = \gcd(b,r)$, where $a = b \cdot q + r$ for some $q \in \mathbb{Z}$, $0 \leq r < b$

A B

Proof: $c \mid a,\ c \mid b \Rightarrow c \mid \underbrace{a \cdot 1 + b(-q)}_{a - bq} \Rightarrow c \mid r$

$A = B \Leftrightarrow \begin{cases} A \geq B \\ B \geq A \end{cases}$

$\Rightarrow \gcd(b, r) \geq \gcd(a, b)$

let $d \mid b,\ d \mid r$

then $d \mid b,\ d \mid b \cdot q + r \Rightarrow d \mid a \Rightarrow \gcd(a,b) \geq \gcd(b,r)$

Euclidean Algorithm

$\gcd(a,b) - ?$

- $a = b q_1 + r_1$ — Lemma: $0 \leq r_1 < b \Rightarrow \gcd(a,b) = \gcd(b, r_1)$
- $b = r_1 q_2 + r_2$ — $0 \leq r_2 < r_1 \Rightarrow \gcd(b, r_1) = \gcd(r_1, r_2)$
- $r_1 = r_2 q_3 + r_3$
- $\vdots$
- $r_{k-2} = r_{k-1} q_k + \boxed{r_k = 0}$ stop

$\gcd(r_k, r_{k-1}) = \gcd(r_{k-1}, r_{k-2})$

$\gcd(0, r_{k-1}) = r_{k-1}$

$\gcd(a,b) = \gcd(0, r_{k-1}) = r_{k-1}$

Ex: $\gcd(60, 37) = 1$

$60 = 37 \cdot 1 + 23$

$37 = 23 \cdot 1 + 14$

$23 = 14 \cdot 1 + 9$

$14 = 9 \cdot 1 + 5$

$9 = 5 \cdot 1 + 4$

$5 = 4 \cdot 1 + \boxed{1}$ ← $\gcd(60, 37)$

$4 = 1 \cdot 4 + 0$

$20212021 = 2021 \cdot 10001 + 0$ (b, r_1, q_2, r_2)

$2021202120212021 = 2021202120212021 \cdot 10000$ (a, q_1)

b | $\boxed{2021}$ ← $r_1 = \gcd$

gcd (12, 10)

$12 = 10 \cdot 1 + 2$ ← gcd ($a = b \cdot q_1 + r_1$)

$10 = 2 \cdot 5 + 0$ ($b = r_1 \cdot q_2 + r_2$)

Theorem: Let $a, b \in \mathbb{Z}$, not both zero.

Then $\gcd(a,b) = \min \{ Xa + Yb \mid X, Y \in \mathbb{Z},\ Xa + Yb > 0 \}$

(smallest number in the set)

Ex: gcd (701, 33)

$701 = 33 \cdot 21 + 8$ ← (693)

$33 = 8 \cdot 4 + 1$ ← gcd ← start

$8 = 1 \cdot 8 + 0$

$1 = 33 - 8 \cdot 4$

$= 33 - (701 - 33 \cdot 21) \cdot 4$

$= 33 - 701 \cdot 4 + 33 \cdot 84$

$= 33 \cdot 85 + 701 \cdot (-4)$

$Y \qquad X$

Def: $a, b \in \mathbb{Z}$ are relatively prime (coprime) if $\gcd(a,b) = 1$.

Lemma: If a, b, c are positive integers, $\gcd(a,b) = 1$ and $a \mid b \cdot c$ then $a \mid c$

Corollary: p is prime if and only if $\forall\ a, b \in \mathbb{Z}$ such that $p \mid a \cdot b$ we must have $p \mid a$ or $p \mid b$

$p \mid a_1 \dots a_n \Rightarrow p \mid a_i$ for some i.

Congruences modulo m

Def: We say that $a \equiv b \pmod m$ if $m \mid (a - b)$

(a congruent to b; $a - b = 0$)

Ex: $14 \equiv 2 \pmod{12}$

$14 = 12 \cdot 1 + 2$

$26 = 12 \cdot 2 + 2$

equivalence class: $1 \quad \{12q + 2\} \quad q \in \mathbb{Z}$

Theorem: If $a \equiv b \pmod c$ and $d \equiv e \pmod c$

Then 1) $a+d \equiv b+e \pmod c$

2) $a \cdot d \equiv b \cdot e \pmod c$

Proof: 1) $(b+e)-(a+d) = b+e-a-b = (b-a)+(e-d)$

$c \mid (b-a)$ $\quad c \mid (e-d)$

$\Rightarrow c \mid b-a+e-d$

2) $a \cdot d - b \cdot e + b \cdot d - b \cdot d$

$= (a-b)d + (d-e)b \longrightarrow c \mid ad - b \cdot e$

$c \mid a-b \qquad c \mid d-e$

"$\equiv$" is an equivalence relation

- $a \equiv a \pmod c$
- $a \equiv b \Rightarrow b \equiv a \pmod c$
- $a \equiv b$, $b \equiv d \pmod c \Rightarrow a \equiv d \pmod c$

Powers of integers modulo prime p

$a \in \mathbb{Z}$, p – prime

$a^1, a^2, a^3, \ldots \pmod p$

Ex: $p=3$, $a=2$

$2^1 = 2 \equiv 2 \pmod 3$

$2^2 = 4 \equiv 1 \pmod 3$

$2^3 = 8 \equiv 2 \pmod 3$

$2^4 = 16 \equiv 1 \ldots$

Ex: $p=5$, $a=2$

$2^1 = 2 \equiv 2 \pmod 5$

$2^2 = 4 \equiv 4 \pmod 5$

$2^3 = 8 \equiv 3$

$2^4 = 16 \equiv 1$

$2^5 = 32 \equiv 2$

$2^6 = 64 \equiv 4$

Ex: $p=7$, $a=3$

$3^1 \equiv 3 \pmod 7$

$3^2 \equiv 2 \pmod 7$

$3^3 \equiv 6$

$3^4 \equiv 4$

$3^5 \equiv 5$

$3^6 \equiv 1$

$3^7 \equiv 3$

$\vdots$

Fermat's Little Theorem Let p be prime, $a \in \mathbb{Z}$, $p \nmid a$

Then $a^{p-1} \equiv 1 \pmod{p}$

Theorem (Wilson) $(n-1)! = (n-1)(n-2)\cdots 3\cdot 2\cdot 1$

$(n-1)! \pmod{n}$?

Ex: $4! = 24 \equiv 4 \pmod 5$ also $24 \equiv -1 \pmod 5$

$6! = 720 \equiv 6 \pmod 7 \equiv -1 \pmod 7$

$10! = 10\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1 \pmod{11}$

$\equiv 5 \pmod 9 \equiv 1 \pmod{11}$ $\equiv 2 \pmod{11}$

$\equiv 10 \pmod{11}$

$\equiv -1 \pmod{11}$

Conjecture: $(n-1)! \overset{?}{\equiv} -1 \pmod n$

$9! = 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1 \equiv 0 \mod (10)$

Theorem: If p is prime then $(p-1)! \equiv -1 \pmod p$

Fermat's Little Theorem Let p be prime, $a \in \mathbb{Z}$, $p \nmid a$

Then $a^{p-1} \equiv 1 \pmod{p}$

Proof: $1, 2, 3, \ldots, p-2, p-1$

multiply by a

Set $\{a, 2a, 3a, \ldots (p-2)a, (p-1)a\}$ reduce $\pmod p$

Ex: $p = 11$, $a = 3$

$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$\times 3$

$\{3, 6, 9, 12, 15, 18, 21, 24, 27, 30\}$

$\pmod{11}$

$\downarrow$

$\{3, 6, 9, 1, 4, 7, 10, 2, 5, 8\}$

Claim: $\{a, 2a, \ldots, (p-1)a\} \pmod p = \{1, 2, \ldots p-1\}$ (up to reordering)

Take: $a \cdot (2a) \cdot (3a) \cdot \ldots \cdot (p-1)a = a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdots (p-1) = a^{p-1} \cdot (p-1)!$

$\equiv (-1) \cdot a^{p-1} \pmod p$

by the claim: $a \cdot (2a) \cdot (3a) \cdots (p-1)a \equiv (p-1)! \pmod p \equiv (-1) \pmod p$

($a \cdot (2a) \cdot (3a) \cdots (p-1)a \equiv (p-1)!$: reduce each $k \cdot a \pmod p$, $1 \le k \le p-1$; $(p-1)! \equiv (-1) \pmod p$: Wilson)

$\Rightarrow a^{p-1}(-1)(-1) \equiv 1 \pmod p \Rightarrow a^{p-1} \equiv 1 \pmod p$

Theorem (Euler) Let $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod p$

$\phi(n)$ – Euler totient function

$\phi(n) = \{$ number of positive integers $\le n$ that are relatively prime to $n\}$

Note: Let p prime $\phi(p) = p-1$, $\gcd(k, p) = 1$, $1 \le k < p$

Euler $\Rightarrow$ FLT

Ex: $3^4 \equiv 1 \pmod{10}$

$\phi(10) = 4$

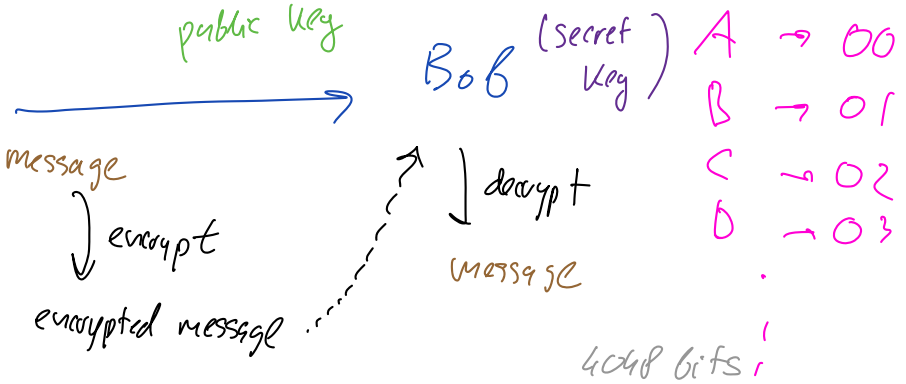
1, 2, 3, 4, 5, 6, 7, 8, 9, 10

Ex: $n = 15$ $\phi(15) = 8$ $2^4 = 16 \equiv 1 \pmod{15}$

$a = 2$ $\gcd(2, 15) = 1$

$2^8 = 256 \equiv 1 \pmod{15}$

RSA:



To decrypt a message you need to factor $N = p \cdot q$ (primes)

RSA works:

$m \in \mathbb{Z}$ - message

A: $m^e \pmod N$ (e ← public) - encrypted message

d - private key

$\varphi(N) = (p-1)\cdot(q-1)$

$e \cdot d \equiv 1 \pmod{\varphi(N)}$

$e \cdot d = 1 + h(p-1)$

$e \cdot d = 1 + \ell(q-1)$ $\quad h, \ell \in \mathbb{Z}$

B: $(m^e)^d = m^{e \cdot d} = m^{e \cdot d - 1} \cdot m$

$= m^{h(p-1)} \cdot m = (m^{p-1})^h \cdot m$

$\equiv 1^h \cdot m \pmod p \equiv m \pmod p$ (FLT)

$m^{ed} = m^{\ell(q-1)} \cdot m = (m^{q-1})^\ell \cdot m \equiv 1^\ell \cdot m \pmod q$ (FLT)

$\equiv m \pmod q$

$m^{e \cdot d} \equiv m \pmod{p \cdot q}$

$\equiv m \pmod N$

Ex: $m = HEY$

07 04 24

$p = 5, \quad q = 7$ (private)

$N = p \cdot q = 35$ (public key)

$\varphi(N) = \varphi(35) = (5-1)\cdot(7-1) = 4 \cdot 6 = 24$

$e = 7 \qquad \gcd(e, \varphi(N)) = 1$

$d \cdot e \equiv 1 \pmod{24}$

$d = 7 \qquad 7 \cdot 7 = 49 \equiv 1 \pmod{24}$

A:

$7^e = 7^7 \equiv 28 \pmod{35}$

$4^e = 4^7 \equiv 4 \pmod{35}$

$24^e = 24^7 \equiv 24 \pmod{35}$

encrypted: 28 04 24

B:

$28^d = 28^7 \equiv 7 \pmod{35}$ H

$4^d = 4^7 \equiv 4 \pmod{35}$ E

$24^d = 24^7 \equiv 24 \pmod{35}$ Y