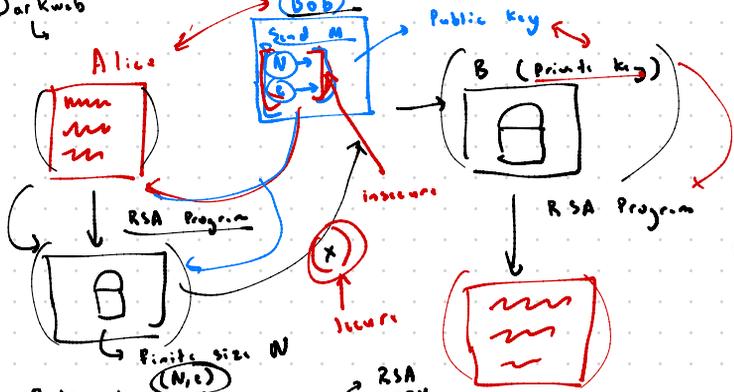
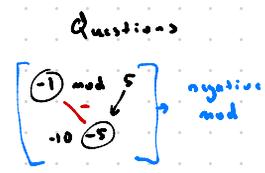
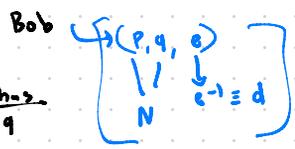


Alice $(N, e) \rightarrow$ Bob's web Eve $\rightarrow (N, e)$

RSA
 ↳ cryptography
 Darkweb
 ↳



name $N=99$
 $\left[\begin{array}{l} d \equiv e^{-1} \pmod{(p-1)(q-1)} \\ (x^e)^d \equiv x \pmod N \end{array} \right]$

Public Key (N, e) large primes 512 bits \rightarrow RSA 1024
 Proof Correctness in notes \rightarrow FLT powerful!
 $(p-1)(q-1)$
 Private Key $d \equiv e^{-1} \pmod{(p-1)(q-1)}$
 inverse \rightarrow Public key

$E(x) = x^e \pmod N$ Alice
 $D(y) = y^d \pmod N$ Bob
 File size N
 (limits) space \rightarrow file size \rightarrow easy calc etc

Eve $(N, e) \rightarrow$ public key
 ↳ knows N, e

↳ not p, q or d if N small \rightarrow all values $x^e \equiv y \pmod N$ is my message
 ↳ (Brute force) $(N$ is huge)
 ↳ needs $p-1, q-1$ \rightarrow needs (p, q) from N
 ↳ prime factoring expensive computationally

Alice Computer $(x^e) \pmod N$ (repeated squaring)

Bob's Computer
 ① $y^d \pmod N$ squares
 ② $e^{-1} \pmod{(p-1)(q-1)}$
 ③ find primes \rightarrow EGCD
 ↳ an algo

Prints $(p, q) \rightarrow N/p \rightarrow q$
 Known inefficient

Binary files (almost impossible)
 $n = m + 5$
 $(x \pmod mn) = m+5x$
 $(5) = \pmod m$
 $(0) = \pmod n$
 $x \pmod mn$
 $\rightarrow x = \begin{bmatrix} n(x) \\ m(x+5) \end{bmatrix}$

$$k_1 \neq k_2 \quad \rightarrow \quad k=1 \quad x=n=m+5$$

$$nk_1 = mk_2 + 5$$

$$x = \begin{pmatrix} n \\ = m+5 \end{pmatrix}$$

1 RSA Warm-Up

Consider an RSA scheme with modulus $N = pq$, where p and q are distinct prime numbers larger than 3.

- (a) What is wrong with using the exponent $e = 2$ in an RSA public key?

what does e need to be for
 d to exist?

- (b) Recall that e must be relatively prime to $p - 1$ and $q - 1$. Find a condition on p and q such that $e = 3$ is a valid exponent.

write p, q in terms of $k \in \mathbb{N}$

- (c) Now suppose that $p = 5$, $q = 17$, and $e = 3$. What is the public key?

- (d) What is the private key?

- (e) Alice wants to send a message $x = 10$ to Bob. What is the encrypted message $E(x)$ she sends using the public key?

don't calc
symbolic using alg we know
as abstract

- (f) Suppose Bob receives the message $y = 24$ from Alice. What equation would he use to decrypt the message? What is the decrypted message?

2 RSA with Multiple Keys → Eve ↳ what techniques → (break code)

Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all of their communications, notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(N_1, e), \dots, (N_k, e)$ where no two N_i 's are the same. Assume that the message is x such that $0 \leq x < N_i$ for every i .

- (a) Suppose Eve sees the public keys $(p_1q_1, 7)$ and $(p_1q_2, 7)$ as well as the corresponding transmissions. Can Eve use this knowledge to break the encryption? If so, how? Assume that Eve cannot compute prime factors efficiently. Think of p_1, q_1, q_2 as massive 1024-bit numbers. Assume p_1, q_1, q_2 are all distinct and are valid primes for RSA to be carried out.

$N_1 = (p_1 \cdot q_1)$ separately
 ↳ (p_1) → doesn't know
 $\gcd(N_1, N_2) = (p_1)$

- (b) The secret society has wised up to Eve and changed their choices of N , in addition to changing their word x . Now, Eve sees keys $(\overbrace{p_1q_1}, N_1), (\overbrace{p_2q_2}, N_2),$ and $(\overbrace{p_3q_3}, N_3)$ along with their trans-

↳ no longer same word
 diff word } $\gcd(\quad) \rightarrow 1$

missions. Argue why Eve cannot break the encryption in the same way as above. Assume $p_1, p_2, p_3, q_1, q_2, q_3$ are all distinct and are valid primes for RSA to be carried out.

- (c) Let's say the secret x was not changed ($e = 3$), so they used the same public keys as before, but did not transmit different messages. How can Eve figure out x ?

3 RSA for Concert Tickets

Alice wants to tell Bob her concert ticket number, m , which is an integer between 0 and 100 inclusive. She wants to tell Bob over an insecure channel that Eve can listen in on, but Alice does not want Eve to know her ticket number.

- (a) Bob announces his public key $(N = pq, e)$, where N is large (512 bits). Alice encrypts her message using RSA. Eve sees the encrypted message, and figures out what Alice's ticket number

is. How did she do it?

- (b) Alice decides to be a bit more elaborate. She picks a random number r that is 256 bits long, so that it is too hard to guess. She encrypts that and sends it to Bob, and also computes rm , encrypts that, and sends it to Bob. Eve is aware of what Alice did, but does not know the value of r . How can she figure out m ?

Answers $(e=2) \rightarrow 2, (p-1)(q-1) \rightarrow p-1, q-1$
 p, q primes
 \Rightarrow odd
 $p-1, q-1 \Rightarrow$ even

a) using e would mean $\gcd(2, (p-1)(q-1)) \neq 1$
 \Rightarrow no inverse d
 p, q prime \Rightarrow odd $\Rightarrow (p-1)(q-1)$ even

b) $(e=3) \Rightarrow \gcd(3, (p-1)(q-1))$
 and $\gcd(3, 2k) = 3$
 $3k+1-1 = 3k$
 $\gcd(3, 3k) = 3$
 \Rightarrow not prime
 small values $\rightarrow [q, p = 3k+2] \quad k \in \mathbb{N}$
 p, q prime

c) $(N=6) \rightarrow N = [pq] \rightarrow$ [factoring]
 $[5, 17, 3] \rightarrow 5 \cdot 17 = 85$
 Public

d) $3d \equiv 1 \pmod{(5-1)(17-1)}$
 $4 \cdot 16 = 64$
 $d \equiv -21 \equiv 43$
 Private

$15 \cdot 10 \rightarrow [150 - 85]$
 $\rightarrow 65$
 $10^2 \cdot 10$

e) $[E(x) = x^3 \pmod{85}] \quad E(10) \equiv 10^3 \equiv 65 \pmod{85}$

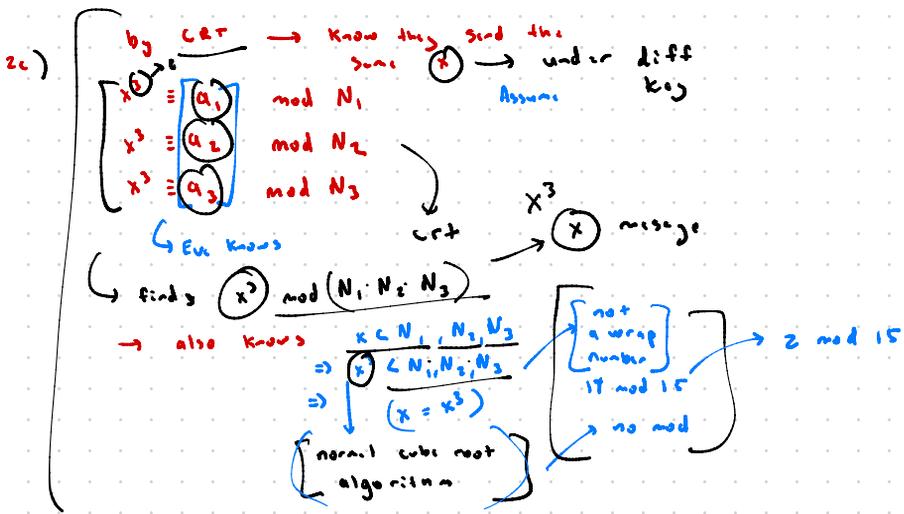
f) $D(y) = y^{43} \pmod{85} \quad D(24) \equiv (24^{43}) \equiv 14 \pmod{85}$
 use this algo
 \hookrightarrow has p, q
 $N \hookrightarrow$ CRT

$24^{43} \equiv (a_1) \pmod{5} \rightarrow 9$
 $24^{43} \equiv (a_2) \pmod{17} \rightarrow 0$
 $b_1 \rightarrow 17^{-1} \pmod{5} \rightarrow 2$
 $b_2 \rightarrow 5^{-1} \pmod{17} \rightarrow 7$
 $24^{43} \equiv a_1 \cdot b_1 \cdot 17 + [a_2 \cdot b_2 \cdot 5] \pmod{85}$
 $\equiv a_1 \pmod{5} \quad \equiv 0 \pmod{17}$

$a_1 = 4, a_2 = 14$
 $b_1 = 3, b_2 = 7$
 $4 \cdot 3 \cdot 17 + 14 \cdot 7 \cdot 5 \pmod{85}$
 $\equiv 14$

2a) Take $(\gcd(p, q_1), p, q_2) = (p_1)$
 \hookrightarrow divides out and get (q_2) or (q_1)
 \rightarrow find $d \equiv e^{-1} \pmod{(p-1)(q-1)}$
 \rightarrow private key
 \rightarrow EGCD
 GCD \rightarrow computationally efficient
 find p_1
 $(2) \quad 7$ or 9 \rightarrow other

2b) No common factors
 \hookrightarrow



2a) Brute Force
only 101 possible m values

2b) $r^c \equiv [y] \pmod{N}$ (with r^c above y)

$$\begin{aligned}
 (m r)^c \pmod{N} &\equiv m^c (r^c) \pmod{N} \\
 &\equiv m^c y \pmod{N}
 \end{aligned}$$

using Extended GCD find $y^{-1} \pmod{N}$ ⇒ (computationally) efficient

$$y^{-1} m^c \equiv m^c \pmod{N}$$

↳ brute force