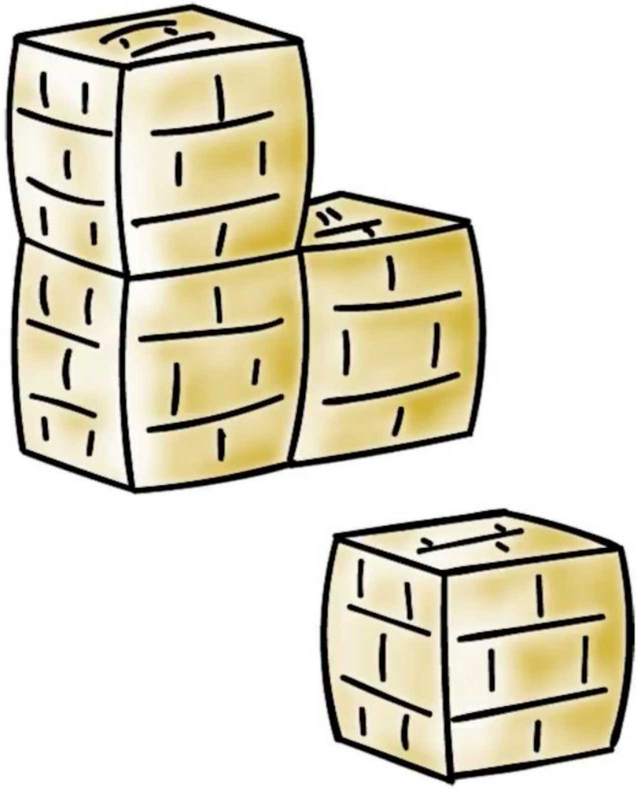
Public Key Algorithms

Lesson Introduction

- Modular arithmetic
- RSA
- Diffie-Hellman

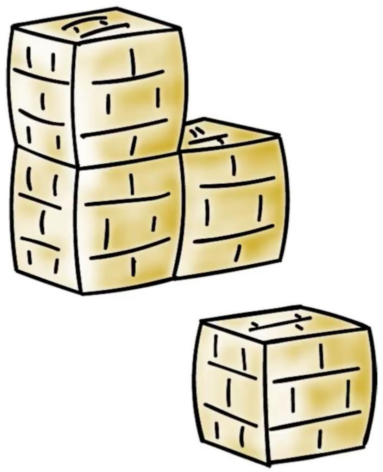
Modular Arithmetic



- **Public key algorithms are based on modular arithmetic**

- Modular addition
- Modular multiplication
- Modular exponentiation

Modular Arithmetic



- **Addition modulo (MOD) *M***
- **Additive inverse:** addition MOD *M* yields 0
  - E.g., M=10, for k=2, its inverse is k^{-1}=8 because 2+8 MOD 10 = 0
- **Reversible:** by adding the inverse
  - Convenient for decryption
  - E.g., for c = 3, p = c+k = 3+2 MOD 10 = 5; p+k^{-1} = 5+8 MOD 10 = 3 = c

Additive Inverse Quiz

What is the additive inverse of 8 MOD 20?

Enter an answer in the textbox:

Modular Multiplication

- **Multiplication modulo M**
- **Multiplicative inverse**: multiplication MOD M yields 1
  - E.g., M=10, 3 and 7 are inverse of each other because $3 \times 7 \text{ MOD } 10 = 1$
- **Only some numbers have inverse**
  - But 2, 5, 6, 8 do not have inverse when M=10

Modular Multiplication

- **Use Euclid's algorithm to find inverse**
  - Given x, n, it finds y such that $x \times y \bmod n = 1$

- **Only the numbers relatively prime to n** has MOD n multiplicative inverse

Modular Multiplication Quiz

What is multiplicative inverse of 3 MOD 17?

Enter an answer in the textbox:

Totient Function

$$\varphi(n)$$

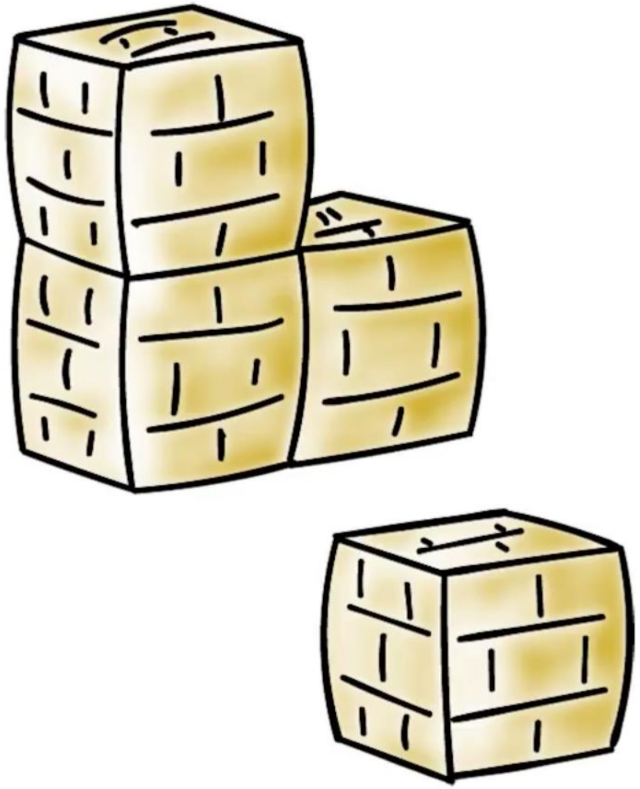
- **x is relatively prime to n**: no common factor other than 1
- **Totient function ø(n):** number of integers smaller than n and relatively prime to n
  - if n is prime, ø(n)=n-1
  - if n=p×q, and p, q are primes, ø(n)=(p-1)(q-1)
  - if n=p×q, and p, q are relative prime to each other, ø(n)=ø(p)ø(q)

Totient Quiz

If n = 21, what is ø(n)?

Enter an answer in the textbox:

Modular Exponentiation



- $x^y \bmod n = x^{y \bmod ø(n)} \bmod n$

- if $y = 1 \bmod ø(n)$ then $x^y \bmod n = x \bmod n$

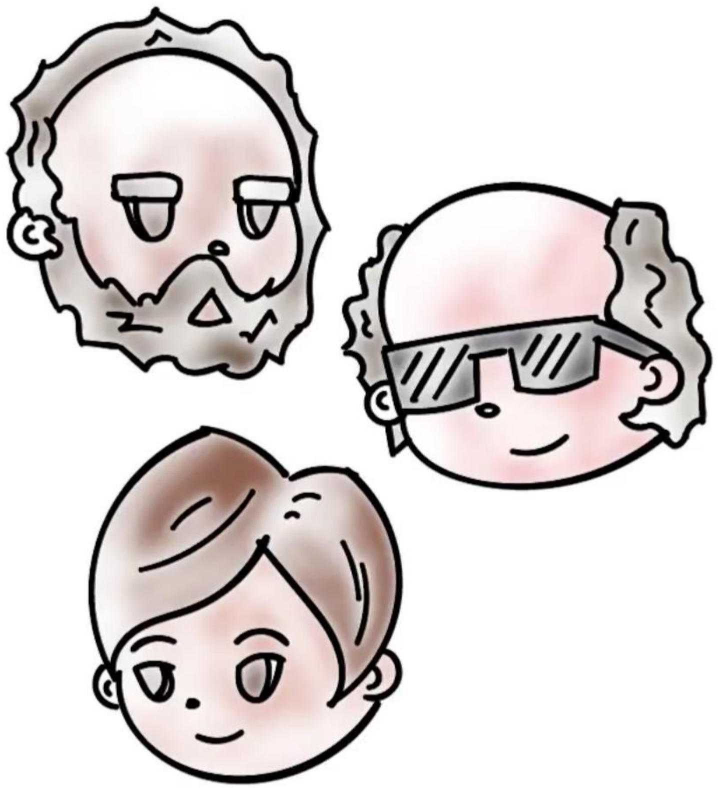
Modular Exponentiation Quiz

Use the totient technique to find c. **Write your answer in the textbox:**

$c = 7^{27} \bmod 30$

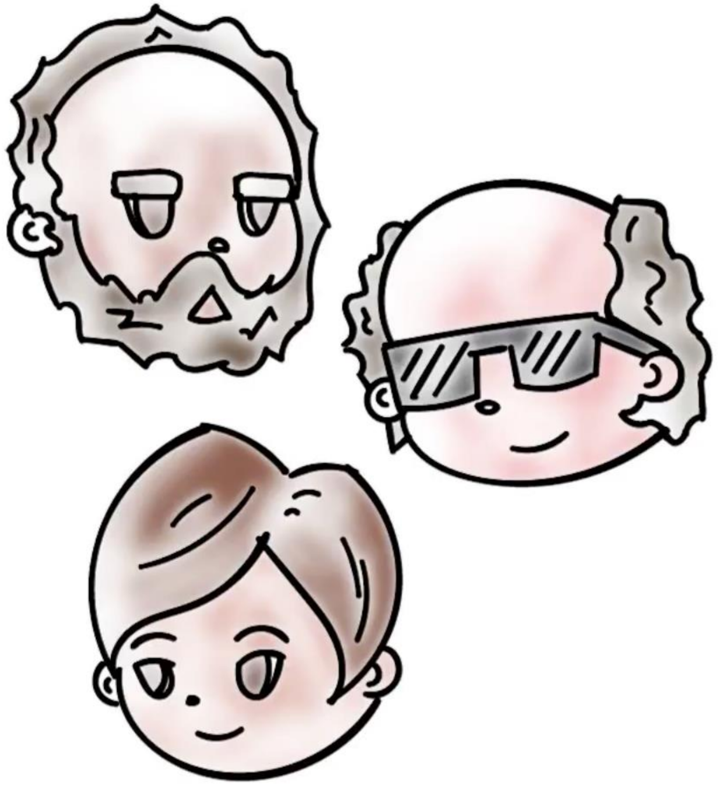
c =

RSA (Rivest, Shamir, Adleman)



- **Widely used**, and one of the first (1977)
- Support both **public key encryption and digital signature**
- **Assumption/theoretical basis:**
  - Factoring a very large integer is hard

RSA Characteristics



- Variable key length
- Variable plaintext block size
  - Plaintext treated as an integer, and must be “smaller” than the key
  - Ciphertext block size is the same as the key length

RSA Algorithm

Key Generation

Select p, q	p and q both prime; $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

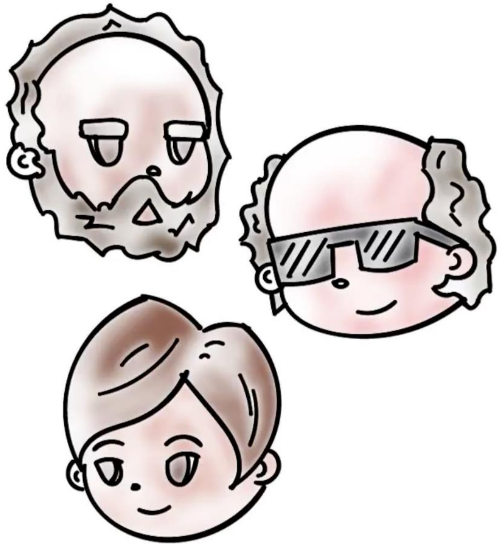
Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

Decryption

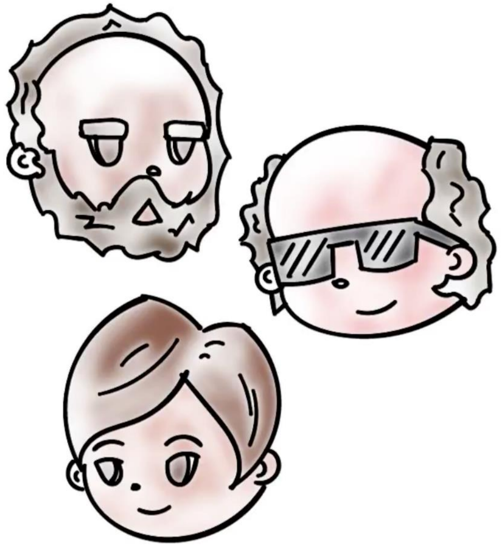
Plaintext:	C
Ciphertext:	$M = C^d \pmod{n}$

How Does RSA Work?



- Given KU = <e, n> and KR = <d, n>
  - **encryption:** $c = m^e \bmod n,\ m < n$
  - **decryption:** $m = c^d \bmod n$
  - **signature:** $s = m^d \bmod n,\ m < n$
  - **verification:** $m = s^e \bmod n$

Why does RSA Work?



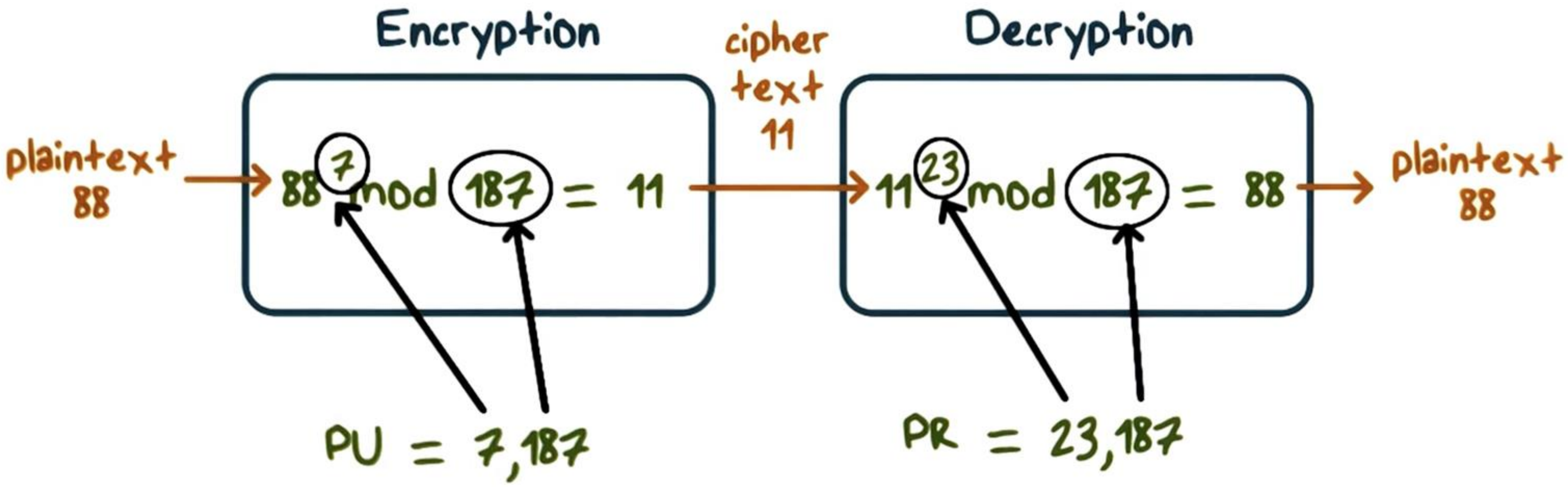
Given pub = <e, n> and priv = <d, n>

- $n = p \times q$, $\varnothing(n) = (p-1)(q-1)$
- $e \times d = 1 \bmod \varnothing(n)$
- $x^{e \times d} = x \bmod n$
- **encryption:** $c = m^e \bmod n$
- **decryption:** $m = c^d \bmod n =$

  $m^{e \times d} \bmod n =$

  $m \bmod n = m$ (since $m < n$)
- digital signature (similar)

Why does RSA Work?



RSA Quiz

Fill in the text boxes:

Given p = 3 and q = 11

1. Compute n: n= $\boxed{}$

2. Compute φ(n):
φ(n) = $\boxed{}$

3. Assume e = 7
Compute the value of d:
d = $\boxed{}$

4. What is the public key

(e,n) = ($\boxed{}$, $\boxed{}$)

5. What is the private key

(d,n) = ($\boxed{}$, $\boxed{}$)

RSA Encryption Quiz

Given:

- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- Message m = 2

What is the encryption of m:

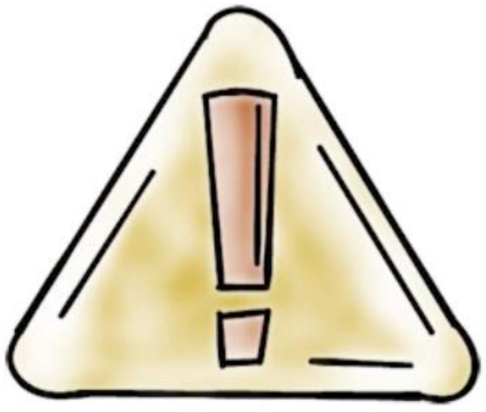
What formula is used to decrypt m?

(Use ** for denoting an exponent)

Why RSA is Secure?

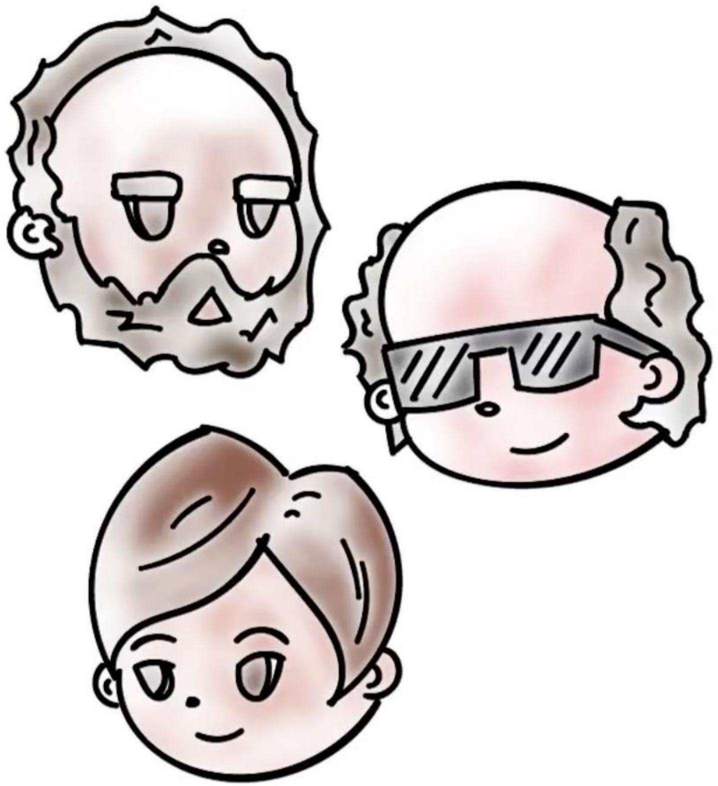
- Factoring an integer with at least 512-bit is **very hard**!
- **But if you can factor big number n then given public key <e,n>, you can find d, and hence the private key by:**
  - Knowing factors p, q, such that, $n = p \times q$
  - Then compute $ø(n) =(p-1)(q-1)$
  - Then find d such that $e \times d = 1 \bmod ø(n)$

RSA in Practice



- Issues with schoolbook RSA
  - **Deterministic:**
    - For the same key, a particular plaintext is always mapped to a particular ciphertext
  - Special-case plaintexts 0, 1, or -1 produce ciphertexts 0, 1, or -1 regardless of keys
  - **Malleable:**
    - Transforming a ciphertext into another leads to predictable transformation to plaintext
      - For $c = m^e \bmod n$, attacker change c to $s^e \times c$
      - Receiver gets $s \times m$ instead of m

RSA in Practice



- **PKCS** (public key cryptography standard) uses **OAEP** (optimal asymmetric encryption padding)
    - Append padding (seeded from random byte) as prefix to m

RSA in Practice Quiz

Select the best answer.

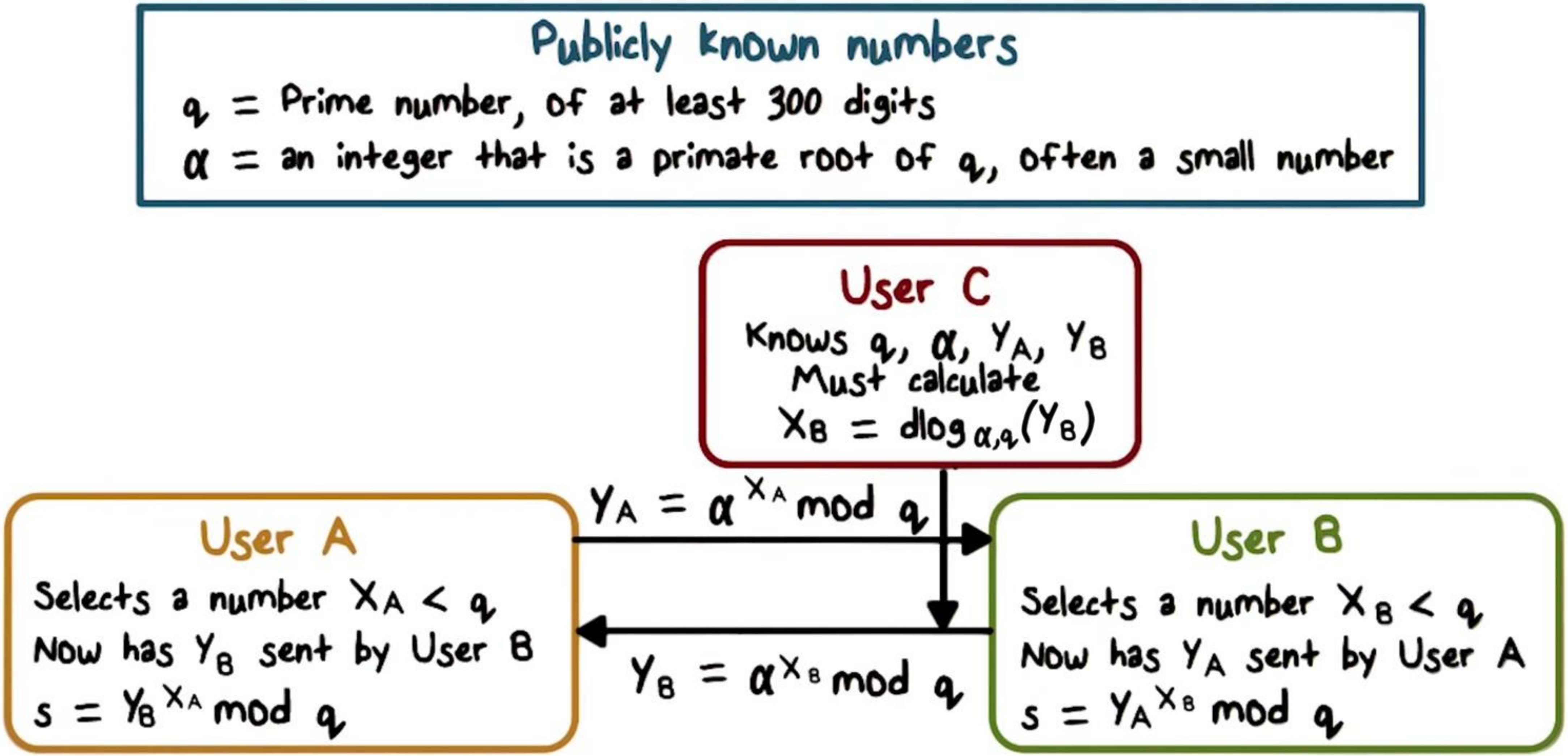
When implementing RSA, it is best to use:

- [ ] Your own custom software, to ensure a secure system
- [ ] Use the standard libraries for RSA

Diffie and Hellman Key Exchange

- **First published** public-key algorithm
- By Diffie and Hellman in 1976 along with the **exposition of public key concepts**
- Used in a number of commercial products
- **Practical method to exchange a secret key** securely that can then be used for subsequent encryption of messages
- Security **relies on difficulty of computing discrete logarithms**

Diffie and Hellman Key Exchange



Diffie-Hellman Example

Have
- Prime number $q = 353$
- Prime number $\alpha = 3$

A and B each computer their public keys
- A computes $Y_A = 3^{97} \bmod 353 = 40$
- B computes $Y_B = 3^{233} \bmod 353 = 248$

Then exchange and computer secret key:
- For A: $K = (Y_B)^{XA} \bmod 353 = 248^{97} \bmod 353 = 160$
- For B: $K = (Y_A)^{XB} \bmod 353 = 40^{233} \bmod 353 = 160$

Attacker must solve:
- $3^{a} \bmod 353 = 40$ which is hard
- Desired answer is 97, then computer key as B does

Diffie-Hellman Quiz

Alice and Bob agree to use
prime q = 23 and primitive root α = 5

Alice chooses secret a = 6
Bob chooses secret b= 15

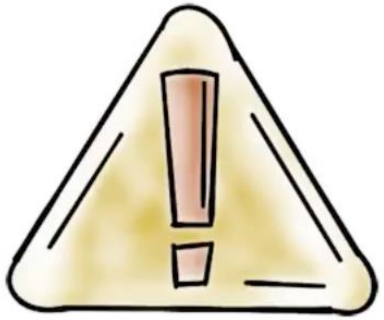
What number does Alice send Bob?

What number does Bob send Alice?

Diffie-Hellman Security

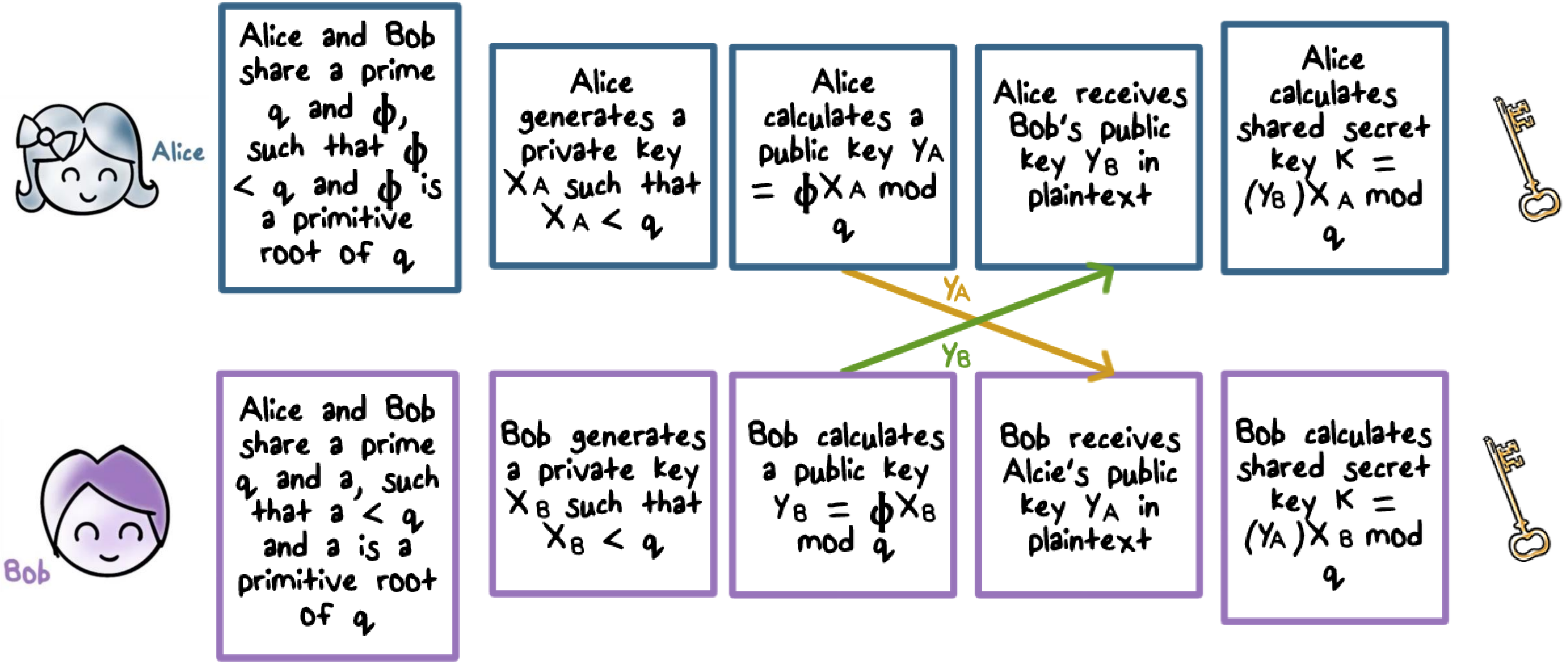
- **Shared key (the secret) itself never transmitted**
- Discrete logarithm is very hard
- $Y = \alpha^X \bmod q$
- **Conjecture:** given Y, α, and q, it is extremely hard to compute the value of X because q is a very large prime (discrete logarithm)

Diffie-Hellman Limitations

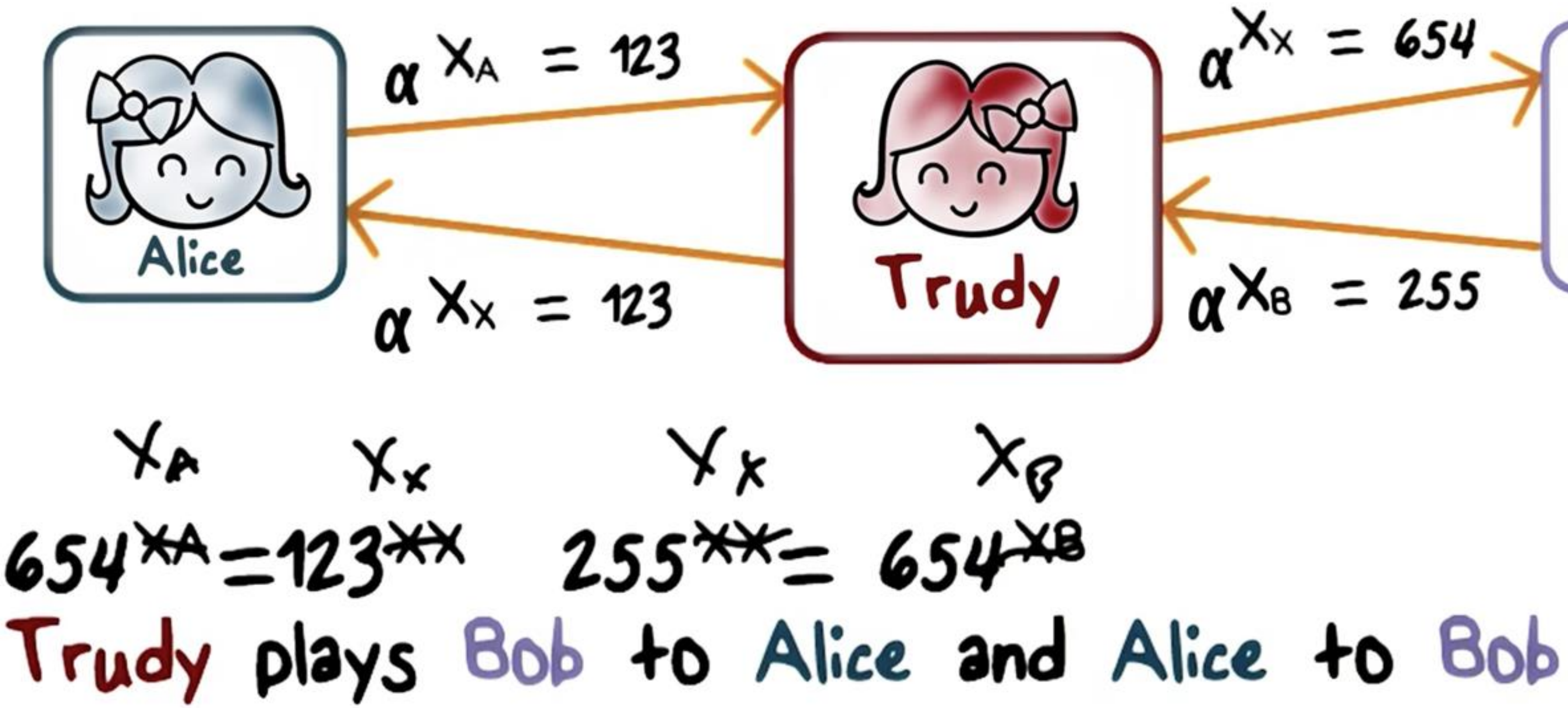


- Expensive exponential operation
    - DoS possible
- The scheme itself **cannot be used to encrypt anything –** it is for secret key establishment
- **No authentication**, so you cannot sign anything

Implementing the Diffie-Hellman Key Exchange



Bucket Brigade Attack, Man-in-the-Middle(MIM)

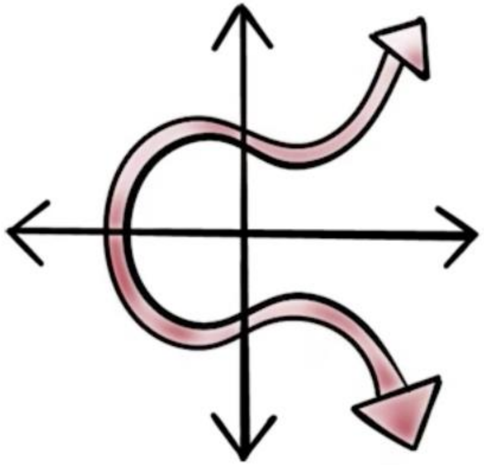


Other Public-Key Algorithms

Digital Signal Standard:

- Makes use of SHA-1 and the Digital Signature Algorithm (DSA)
- Originally proposed in 1991, revised in 1993 due to security concerns, and another minor revision in 1996
- **Cannot be used for encryption or key exchange**
- Uses an algorithm that is designed to provide only the digital signature function

Other Public-Key Algorithms



Elliptic-Curve Cryptography (ECC):

- Equal security for smaller bit size than RSA
- Seen in standards such as IEEE P1363
- Confidence level in ECC is not yet as high as that in RSA
- **Based on a mathematical construct known as the elliptic curve**

RSA, Diffie-Hellman Quiz

Check the statements that are True:

- [ ] RSA is a block cipher in which the plaintext and ciphertext are integers between 0 and $n - 1$ for some n
- [ ] If someone invents a very efficient method to factor large integers, then RSA becomes insecure
- [ ] The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms
- [ ] The Diffie-Hellman key exchange protocol is vulnerable to a man-in-the-middle attack because it does not authenticate the participants
- [ ] RSA and Diffie-Hellman are the only public-key algorithms

Public Key Algorithms
Lesson Summary

- Modular arithmetic the foundations of several public key algorithms
- RSA can be used for encryption and signature, its security is based on assumption that factoring a larger integer into two primes is hard
- Diffie-Hellman is used for key exchange, its security is based on the assumption that discrete logarithm on large numbers is hard
  - No authentication means man-in-the-middle attack possible