Lec 10: Cryptography (2)

CSED415: Computer Security

Spring 2024

Seulbae Kim

POSTECH

POHANG UNIVERSITY OF SCIENCE AND TECHNOLOGY

Administrivia

- Lab 02 deadline is fast approaching
  - Due Sunday, March 24

- Check lecture follow-ups!

5Week [18 March - 24 March]

[Slides] Lec 09: Cryptography (1) 1.9MB PDF document

Typo fixed on page 48: psuedorandom -> pseudorandom

Lec 09 Follow-up

Cryptography roadmap

Goal \ Scheme	Symmetric Key	Asymmetric Key
Confidentiality	✅ One Time Pad (OTP) ✅ Block ciphers (DES, AES) ✅ Stream ciphers	• ElGamal encryption • RSA encryption
Integrity & Authentication	• Message Authentication Code (MAC)	• Digital signature

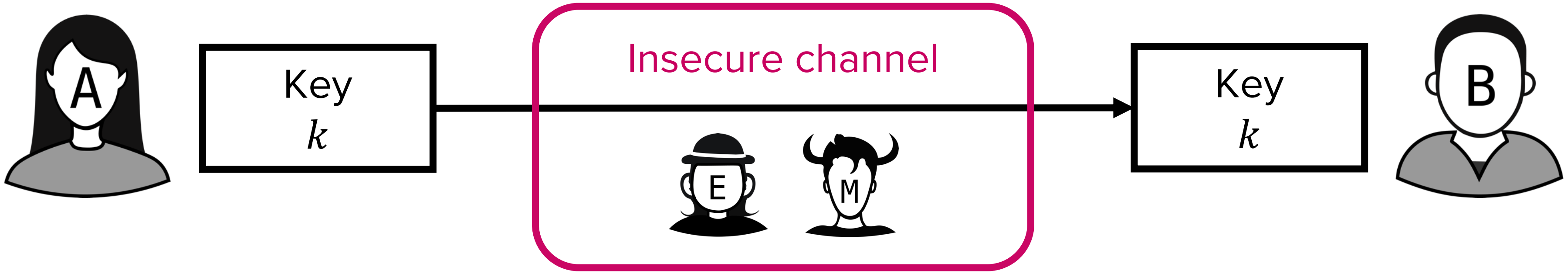
Tools

- Secure key exchange
- Hash

Secure Key Exchange

Limitation of symmetric key scheme

- Symmetric key cryptography requires key k to be securely shared between Alice and Bob
- For securely sharing messages over insecure channels, symmetric key cryptography is used
- However, symmetric schemes do not work without k



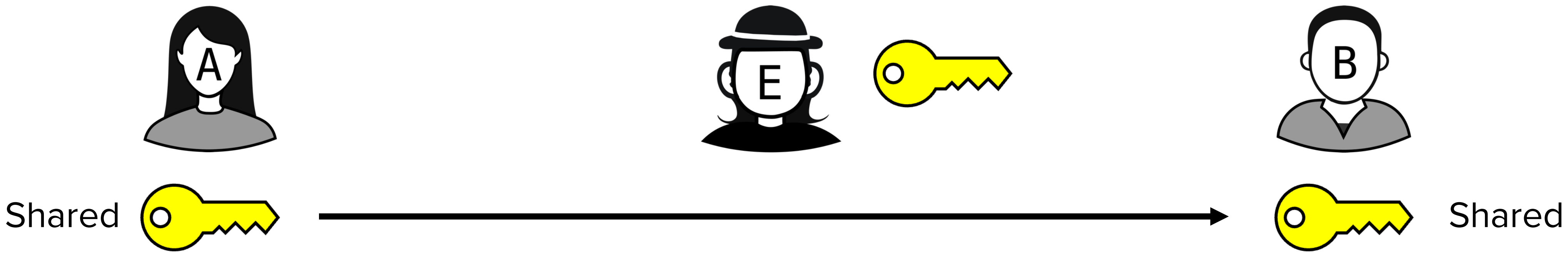
A secure key exchange algorithm is needed

Diffie-Hellman key exchange

- Named after Whitfield Diffie and Martin Hellman
- Idea: Share a key without sharing it
  - Mathematically derive a synchronized key rather than sharing a key

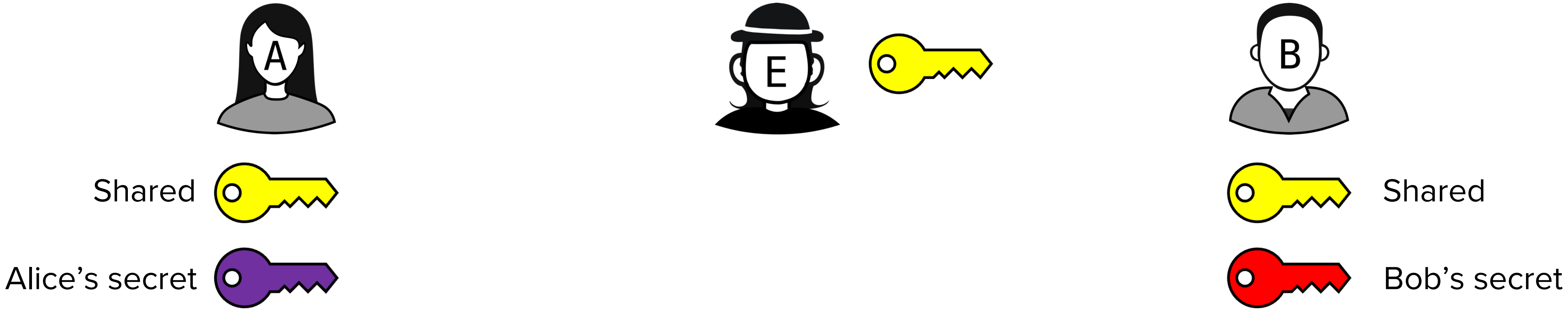
Intuitive example: Colored keys

1. Alice shares a yellow key to Bob (and Eve)



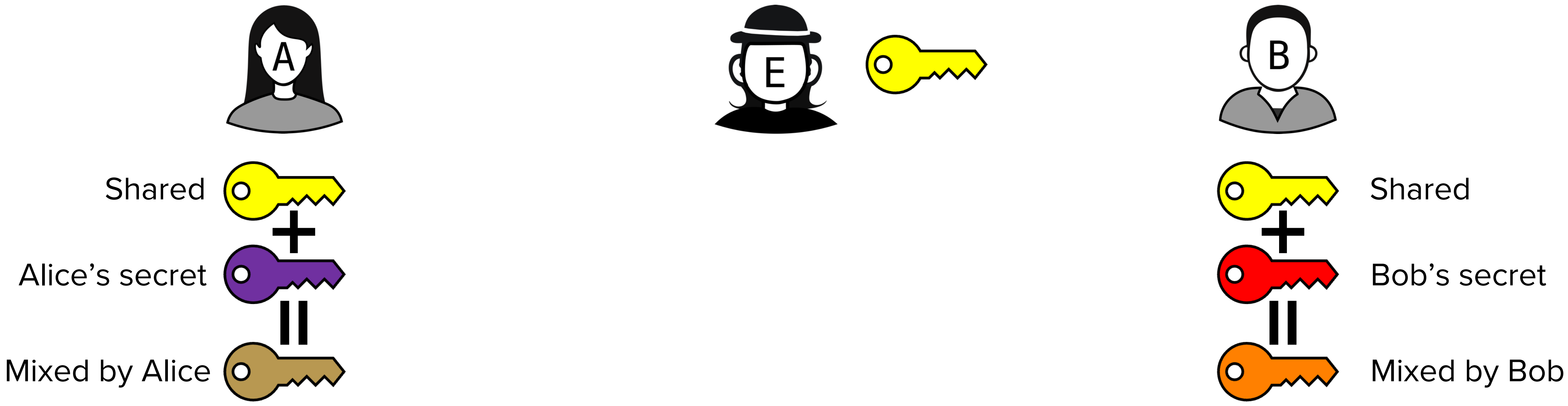
Intuitive example: Colored keys

2. Alice and bob each select a colored key and keep it to themselves, respectively



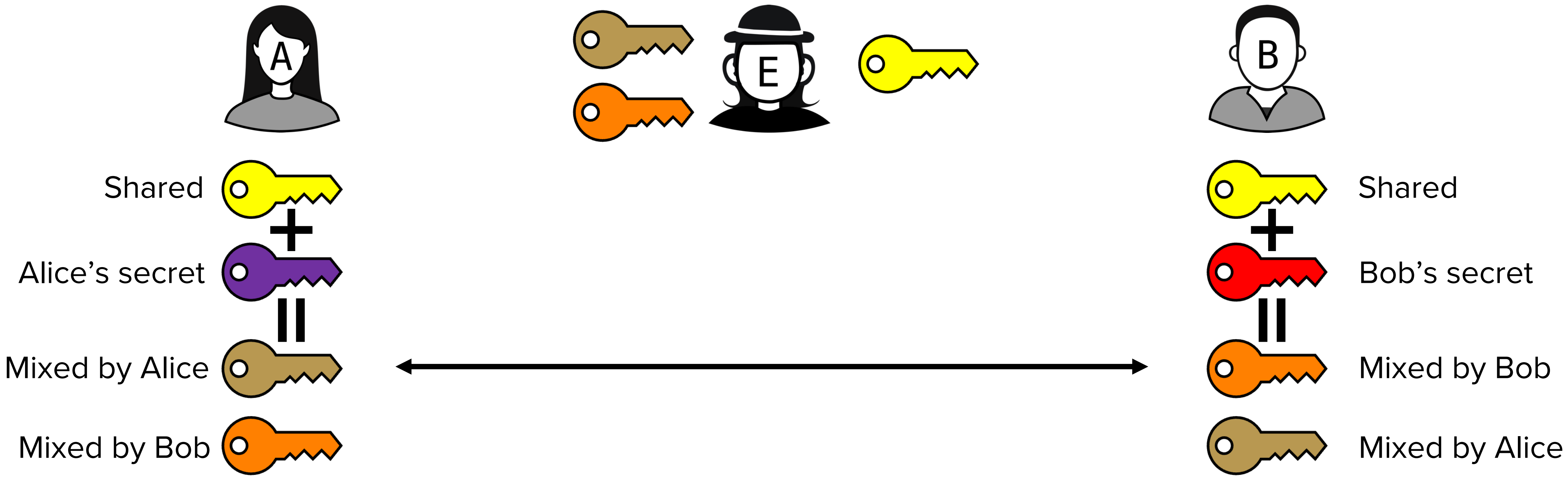
Intuitive example: Colored keys

3. Alice and bob mix the color of the keys



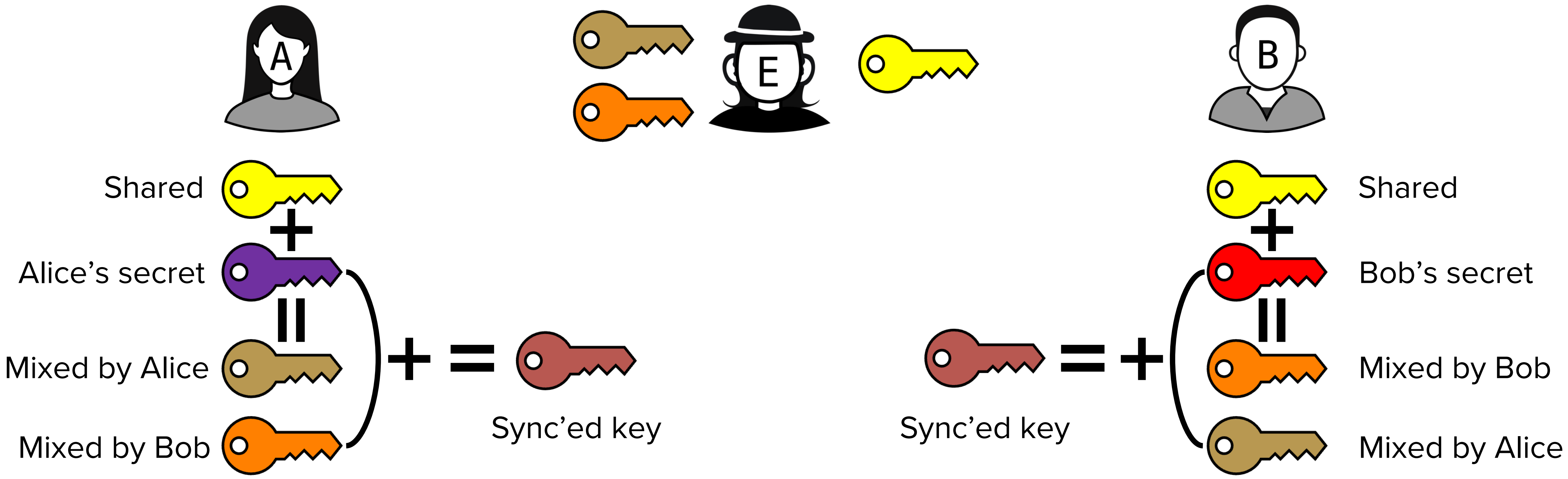
Intuitive example: Colored keys

4. Alice and bob share the mixed keys to each other (and Eve)



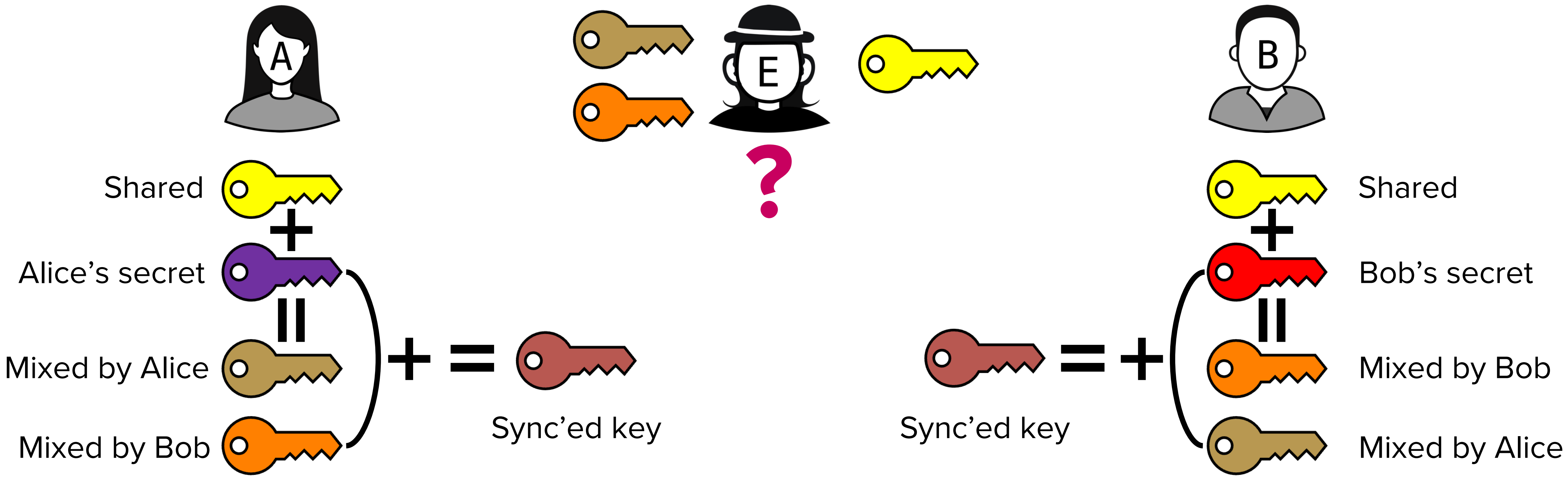
Intuitive example: Colored keys

5. Alice and bob mix the color of received mixed key with their secret keys



Intuitive example: Colored keys

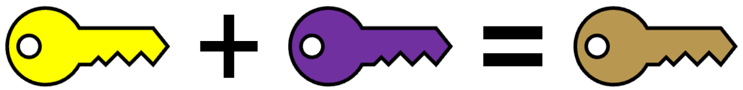
6. Eve cannot derive the sync'ed key without knowing Alice's or Bob's secret keys

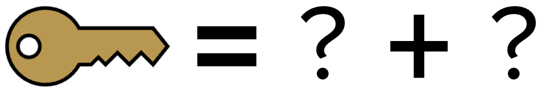


Intuitive example: Colored keys

6. Eve cannot derive the sync'ed key without knowing Alice's or Bob's secret keys

Some procedures are easy in one direction and hard in the other

Easy: 

Hard: 

Mixed by Bob

Sync'ed key

Sync'ed key

Mixed by Alice

Background: Number theory

- Greatest common denominator $d = \gcd(a, b)$:
  - Largest integer d such that d divides a and d divides b
- Relatively prime (or, Coprime)
  - If $\gcd(a, b) = 1$, then a and b are relatively prime
    - Is 15 relatively prime to 28? Yes. $\gcd(15,28) = 1$
    - Is 14 and 49 relatively prime? No. $\gcd(14,49) = 7$
    - Are 23 and 443 coprime? Yes. Two prime numbers are always coprime
      - Hint: 23 and 443 are prime numbers

Background: Number theory

- $\mathbb{Z}_N = \{0, 1, 2, \dots, N-1\}$
  - Contains all the integers that are possible values of $a \; mod \; N$
  - e.g., $\mathbb{Z}_{12} = \{0, 1, 2, \dots, 11\}$ // possible remainders of dividing int by 12
- $\mathbb{Z}_N^* = \{i \in \mathbb{Z}_N : \gcd(i, N) = 1\}$
  - Contains all elements in $\mathbb{Z}_N$ that are relatively prime to N
  - e.g., $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$
    - $\gcd(1, 12) = \gcd(5, 12) = \gcd(7, 12) = \gcd(11, 12) = 1$
- $\varphi(N) = |\mathbb{Z}_N^*|$
  - Totient function: Number of elements in $\mathbb{Z}_N^*$. e.g., $\varphi(12) = |\mathbb{Z}_{12}^*| = 4$

Background: Number theory

- Generator g
  - An integer such that every integer relatively prime to p can be expressed as a power of $g \ mod \ p$
  - In other words, g generates all the elements in the set $\mathbb{Z}_p^*$
  - Example: Find a generator for $p = 11$
    - $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

i	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
$2^i \ mod \ 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \ mod \ 11$	1	5	3	4	9	1	5	3	4	9	1

    - $g = 2$ is a generator. $g = 5$ is not.

Background: Number theory

- Number of generators
  - For a prime p, the number of generators is $\varphi(p-1)$
  - Example: Find the number of generators for $p = 11$
    - $\mathbb{Z}_{p-1}^* = \mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$
    - $\varphi(p-1) = |\mathbb{Z}_{10}^*| = 4$
    - Thus, there are 4 generators for $p = 11$

Diffie-Hellman key exchange

1. Choose a prime number p and its generator g such that $g < p$
   - Assume $p = 11$
   - $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

	i	0	1	2	3	4	5	6	7	8	9	10	gen?
	$2^i \ mod\ 11$	1	2	4	8	5	10	9	7	3	6	1	Y
	$3^i \ mod\ 11$	1	3	9	5	4	1	3	9	5	4	1	N
	$4^i \ mod\ 11$	1	4	5	9	3	1	4	5	9	3	1	N
	$5^i \ mod\ 11$	1	5	3	4	9	1	5	3	4	9	1	N
$g = 6$ →	$6^i \ mod\ 11$	1	6	3	7	9	10	5	8	4	2	1	Y
	…												

Diffie-Hellman key exchange

2. Alice and Bob each choose a secret key
   - Assume Alice's secret key $a = 15$ and Bob's secret key $b = 8$

Public	Secret
$p = 11$	$a = 15$
$g = 6$	$b = 8$

Diffie-Hellman key exchange

2. Alice and Bob each choose a secret key
   - Assume Alice's secret key $a = 15$ and Bob's secret key $b = 8$

Public	Secret
$p = 11$	$a = 15$
$g = 6$	$b = 8$

3. Alice and Bob compute $g^x \ mod \ p$ where x is the secret key
   - $A = 6^{15} \ mod \ 11$
   - $B = 6^8 \ mod \ 11$

← Too large to be calculated by hand?

Diffie-Hellman key exchange

- Modular exponentiation
  - We can compute $x^y \; mod \; n$ by breaking y down into powers of 2
  - e.g., $6^{15} \; mod \; 11$ → 15 = 8 + 4 + 2 + 1
    - $6^{15} = 6^8 \times 6^4 \times 6^2 \times 6$
    - $6 \; mod \; 11 = 6$
    - $6^2 \; mod \; 11 = 36 \; mod \; 11 = 3$
    - $6^4 \; mod \; 11 = (6^2)^2 \; mod \; 11 = 3^2 \; mod \; 11 = 9$
    - $6^8 \; mod \; 11 = (6^4)^2 \; mod \; 11 = 9^2 \; mod \; 11 = 81 \; mod \; 11 = 4$
    - Thus, $6^{15} \; mod \; 11 = (4 \times 9 \times 3 \times 6) \; mod \; 11 = 648 \; mod \; 11 = 10$

Diffie-Hellman key exchange

2. Alice and Bob each choose a secret key
   - Assume Alice's secret key $a = 15$ and Bob's secret key $b = 8$

Public	Secret
$p = 11$	$a = 15$
$g = 6$	$b = 8$

3. Alice and Bob compute $g^x \mod p$ where x is the secret key
   - Alice's mixed key $A = 6^{15} \mod 11 = 10$
   - Bob's mixed key $B = 6^8 \mod 11 = 4$

Diffie-Hellman key exchange

4. Alice and Bob exchange their mixed keys
   - $A = 6^{15}\ mod\ 11 = 10$
   - $B = 6^{8}\ mod\ 11 = 4$

Public	Secret
$p = 11$	$a = 15$
$g = 6$	$b = 8$
$A = 10$	
$B = 4$	

Diffie-Hellman key exchange

5. Alice and Bob generate a shared key k using the exchanged mixed key and their secret keys
   - Alice: $k = B^a \, mod \, p = 4^{15} \, mod \, 11$
   - Bob: $k = A^b \, mod \, p = 10^8 \, mod \, 11$

Public	Secret
$p = 11$	$a = 15$
$g = 6$	$b = 8$
$A = 10$	
$B = 4$	

Diffie-Hellman key exchange

5. Alice and Bob generate a shared key k using the exchanged mixed key and their secret keys
    - Alice: $k = B^a \mod p = 4^{15} \mod 11$
    - Bob: $k = A^b \mod p = 10^8 \mod 11$

$$4^{15} \mod 11 = 4^8 \times 4^4 \times 4^2 \times 4 \mod 11$$

Public	Secret
$p = 11$	$a = 15$
$g = 6$	$b = 8$
$A = 10$	
$B = 4$	

Diffie-Hellman key exchange

5. Alice and Bob generate a shared key k using the exchanged mixed key and their secret keys
   - Alice: $k = B^a \; mod \; p = 4^{15} \; mod \; 11$
   - Bob: $k = A^b \; mod \; p = 10^8 \; mod \; 11$

Public	Secret
$p = 11$	$a = 15$
$g = 6$	$b = 8$
$A = 10$	
$B = 4$	

$$4^{15} \; mod \; 11 = 4^8 \times 4^4 \times 4^2 \times 4 \; mod \; 11$$

$$4 \; mod \; 11 = 4$$
$$4^2 \; mod \; 11 = 16 \; mod \; 11 = 5$$
$$4^4 \; mod \; 11 = (4^2)^2 \; mod \; 11 = 5^2 \; mod \; 11 = 25 \; mod \; 11 = 3$$
$$4^8 \; mod \; 11 = (4^4)^2 \; mod \; 11 = 9 \; mod \; 11 = 9$$

Diffie-Hellman key exchange

5. Alice and Bob generate a shared key k using the exchanged mixed key and their secret keys
   - Alice: $k = B^a \, mod \, p = 4^{15} \, mod \, 11 = 1$
   - Bob: $k = A^b \, mod \, p = 10^8 \, mod \, 11$

Public	Secret
$p = 11$	$a = 15$
$g = 6$	$b = 8$
$A = 10$	
$B = 4$	

$$4^{15} \, mod \, 11 = 4^8 \times 4^4 \times 4^2 \times 4 \, mod \, 11 = 9 \times 3 \times 5 \times 4 \, mod \, 11 = 1$$

$$4 \, mod \, 11 = 4$$
$$4^2 \, mod \, 11 = 16 \, mod \, 11 = 5$$
$$4^4 \, mod \, 11 = (4^2)^2 \, mod \, 11 = 5^2 \, mod \, 11 = 25 \, mod \, 11 = 3$$
$$4^8 \, mod \, 11 = (4^4)^2 \, mod \, 11 = 9 \, mod \, 11 = 9$$

Diffie-Hellman key exchange

5. Alice and Bob generate a shared key k using the exchanged mixed key and their secret keys
   - Alice: $k = B^a \; mod \; p = 4^{15} \; mod \; 11 = 1$
   - Bob: $k = A^b \; mod \; p = 10^8 \; mod \; 11 = 1$

$10 \; mod \; 11 \equiv -1 \; mod \; 11$
$10^8 \; mod \; 11 = (-1)^8 \; mod \; 11 = 1 \; mod \; 11 = 1$

Public	Secret
$p = 11$	$a = 15$
$g = 6$	$b = 8$
$A = 10$	
$B = 4$	

Diffie-Hellman key exchange

5. Alice and Bob generate a shared key k using the exchanged mixed key and their secret keys
   - Alice: $k = B^a \; mod \; p = 4^{15} \; mod \; 11 = 1$
   - Bob: $k = A^b \; mod \; p = 10^8 \; mod \; 11 = 1$

Public	Secret
$p = 11$	$a = 15$
$g = 6$	$b = 8$
$A = 10$	$k = 1$
$B = 4$	

Alice and Bob have successfully generated a shared key

Diffie-Hellman key exchange

- Can Eve deduce the shared key?
  - Find a and b and k such that
    $A^b \; mod \; 11 = \mathrm{B^a} \bmod 11 = \mathrm{k}$
    where $A = 10$ and $B = 4$?
  - Eve knows the algorithm, i.e.,
    - $6^a \; mod \; 11 = 10$ and $6^b \; mod \; 11 = 4$

Public	Secret
$p = 11$	$a = 15$
$g = 6$	$b = 8$
$A = 10$	$k = 1$
$B = 4$	

Discrete log problem:
"Given p, g, and $g^a \; mod \; p$, it is computationally difficult to find a, especially for large prime number p"

Generalization of Diffie-Hellman key exchange

- A large prime p and a generator g is given
- Alice chooses a secret integer a and computes $A = g^a \: mod \: p$
- Bob chooses a secret integer b and computes $B = g^b \: mod \: p$

Generalization of Diffie-Hellman key exchange

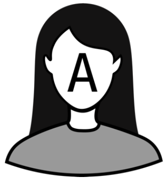
- A large prime p and a generator g is given
- Alice chooses a secret integer a and computes $A = g^a \, mod \, p$
- Bob chooses a secret integer b and computes $B = g^b \, mod \, p$
- Alice computes $k = B^a \, mod \, p = \left(g^b\right)^a mod \, p = g^{ab} \, mod \, p$
- Bob computes $k = A^b \, mod \, p = (g^a)^b \, mod \, p = g^{ab} \, mod \, p$

Generalization of Diffie-Hellman key exchange

- A large prime p and a generator g is given
- Alice chooses a secret integer a and computes $A = g^a \, mod \, p$
- Bob chooses a secret integer b and computes $B = g^b \, mod \, p$
- Alice computes $k = B^a \, mod \, p = \left(g^b\right)^a mod \, p = g^{ab} \, mod \, p$
- Bob computes $k = A^b \, mod \, p = (g^a)^b \, mod \, p = g^{ab} \, mod \, p$
- Eve knows p, g, A, and B
  - Due to discrete log problem, Eve cannot compute a nor b if p is large
  - DH key exchange is secure against passive attacks

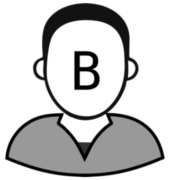
Diffie-Hellman key exchange

- Intended key exchange



Select a
Compute $g^{a}\ mod\ p$

Receive $g^{b}\ mod\ p$
Compute $(\mathrm{g}^{\mathrm{b}})^{\mathrm{a}}\ mod\ p$

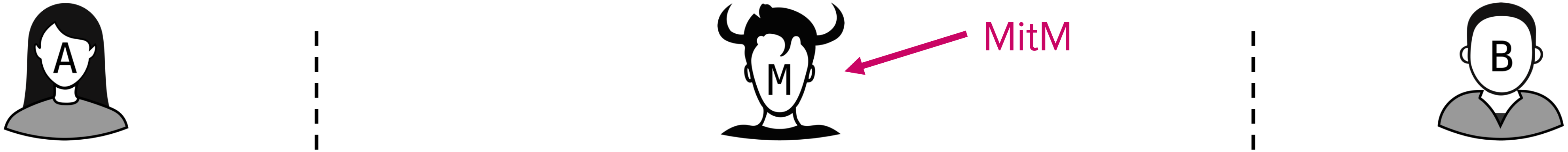


Select b
Compute $g^{b}\ mod\ p$

Receive $g^{a}\ mod\ p$
Compute $(\mathrm{g}^{\mathrm{a}})^{\mathrm{b}}\ mod\ p$

Diffie-Hellman – Man in the Middle (MitM) attack

- What if Mallory actively changes key exchange messages?



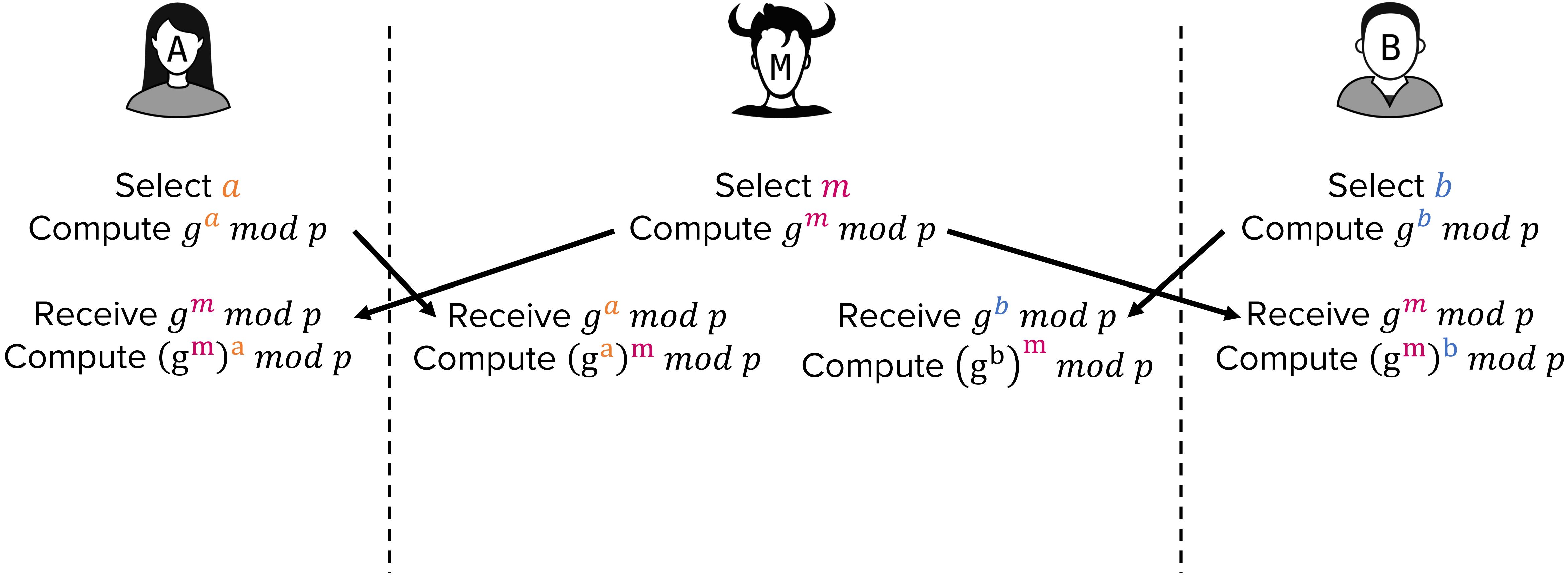
Select a
Compute $g^a \ mod \ p$

Select m
Compute $g^m \ mod \ p$

Select b
Compute $g^b \ mod \ p$

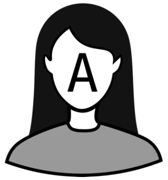
Diffie-Hellman – Man in the Middle (MitM) attack

- What if Mallory actively changes key exchange messages?



Diffie-Hellman – Man in the Middle (MitM) attack

- What if Mallory actively changes key exchange messages?



Select a
Compute $g^a \, mod \, p$

Receive $g^m \, mod \, p$
Compute $(\mathrm{g}^{\mathrm{m}})^{\mathrm{a}} \, mod \, p$

$k = g^{ma} \, mod \, p$

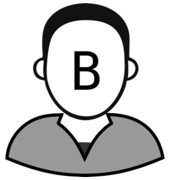
Select m
Compute $g^m \, mod \, p$

Receive $g^a \, mod \, p$
Compute $(\mathrm{g}^{\mathrm{a}})^{\mathrm{m}} \, mod \, p$

$k = g^{ma} \, mod \, p$

Receive $g^b \, mod \, p$
Compute $\left(\mathrm{g}^{\mathrm{b}}\right)^{\mathrm{m}} \, mod \, p$

$k' = g^{mb} \, mod \, p$



Select b
Compute $g^b \, mod \, p$

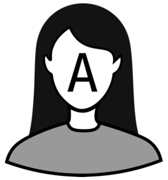
Receive $g^m \, mod \, p$
Compute $(\mathrm{g}^{\mathrm{m}})^{\mathrm{b}} \, mod \, p$

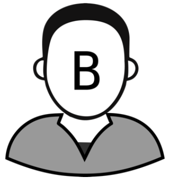
$k' = g^{mb} \, mod \, p$

Mallory keeps two shared keys, k for Alice and k’ for Bob

Diffie-Hellman – Man in the Middle (MitM) attack

- What if Mallory actively changes key exchange messages?





Alice:

Select a
Compute $g^a \bmod p$

Receive $g^m \bmod p$
Compute $(g^m)^a \bmod p$

$k = g^{ma} \bmod p$

$E(k, msg)$

Mallory:

Select m
Compute $g^m \bmod p$

Receive $g^a \bmod p$
Compute $(g^a)^m \bmod p$

$k = g^{ma} \bmod p$

$D(k, E(k, msg))$

Receive $g^b \bmod p$
Compute $(g^b)^m \bmod p$

$k' = g^{mb} \bmod p$

Bob:

Select b
Compute $g^b \bmod p$

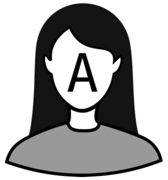
Receive $g^m \bmod p$
Compute $(g^m)^b \bmod p$

$k' = g^{mb} \bmod p$

Mallory can decrypt Alice's msg using k

Diffie-Hellman – Man in the Middle (MitM) attack

- What if Mallory actively changes key exchange messages?



Select a
Compute $g^{a}\ mod\ p$

Receive $g^{m}\ mod\ p$
Compute $(g^{m})^{a}\ mod\ p$

$k = g^{ma}\ mod\ p$

$E(k, msg)$

Select m
Compute $g^{m}\ mod\ p$

Receive $g^{a}\ mod\ p$
Compute $(g^{a})^{m}\ mod\ p$

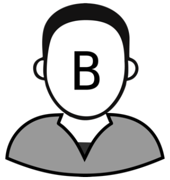
$k = g^{ma}\ mod\ p$

$D(k, E(k, msg))$

Receive $g^{b}\ mod\ p$
Compute $(g^{b})^{m}\ mod\ p$

$k' = g^{mb}\ mod\ p$

$E(k', msg')$



Select b
Compute $g^{b}\ mod\ p$

Receive $g^{m}\ mod\ p$
Compute $(g^{m})^{b}\ mod\ p$

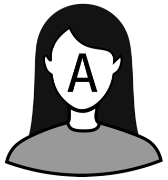
$k' = g^{mb}\ mod\ p$

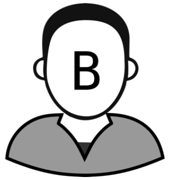
$D(k', E(k', msg'))$

Mallory can modify the msg and encrypt it using k'

Diffie-Hellman – Man in the Middle (MitM) attack

- What if Mallory actively changes key exchange messages?





Select a
Compute $g^a \ mod \ p$

Receive $g^m \ mod \ p$
Compute $(\mathrm{g}^{\mathrm{m}})^{\mathrm{a}} \ mod \ p$

$k = g^{ma} \ mod \ p$

$E(k, msg)$

Select m
Compute $g^m \ mod \ p$

Receive $g^a \ mod \ p$
Compute $(\mathrm{g}^{\mathrm{a}})^{\mathrm{m}} \ mod \ p$

$k = g^{ma} \ mod \ p$

$\mathrm{D}(k, E(k, msg))$

Receive $g^b \ mod \ p$
Compute $\left(\mathrm{g}^{\mathrm{b}}\right)^{\mathrm{m}} \ mod \ p$

$k' = g^{mb} \ mod \ p$

$E(k', msg')$

Select b
Compute $g^b \ mod \ p$

Receive $g^m \ mod \ p$
Compute $(\mathrm{g}^{\mathrm{m}})^{\mathrm{b}} \ mod \ p$

$k' = g^{mb} \ mod \ p$

$D(k', E(k', msg'))$

Alice and Bob think they are securely communicating

Diffie-Hellman – Man in the Middle (MitM) attack

- What if Mallory actively changes key exchange messages?

DH key exchange is insecure against active attacks

$k = g^{ma} \bmod p$ | $k = g^{ma} \bmod p$ | $k' = g^{mb} \bmod p$ | $k' = g^{mb} \bmod p$

$E(k, msg) \rightarrow D(k, E(k, msg))$ | $E(k', msg') \rightarrow D(k', E(k', msg'))$

Alice and Bob think they are securely communicating

Key exchange in the presence of active attacker

- When Mallory (an active attacker) is present, it is impossible for Alice and Bob to start from scratch and exchange messages to derive a shared key unknown to the adversary
- Why?
  - There is no way for Bob to distinguish Alice from Mallory (DH does not provide authentication)
- Alice and Bob needs some "information advantage" over the adversary
  - Typically, in the form of long-lived keys (e.g., previously shared keys)

Cryptography roadmap

Goal \ Scheme	Symmetric Key	Asymmetric Key
Confidentiality	✅ One Time Pad (OTP) ✅ Block ciphers (DES, AES) ✅ Stream ciphers	• ElGamal encryption • RSA encryption
Integrity & Authentication	• Message Authentication Code (MAC)	• Digital signature

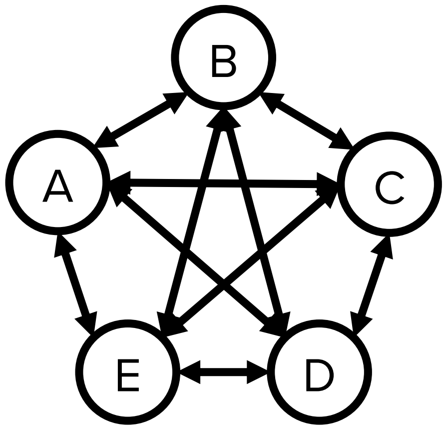
Tools

✅ Secure key exchange
- Hash

Asymmetric Cryptography (Public key Scheme)

Motivation

- More limitations of symmetric key schemes
  - Number of keys needed



→ $\binom{n}{2} = \frac{n(n-1)}{2}$ keys are needed for n people to securely communicate using symmetric schemes

Brief history of public key cryptography

- Whitfield Diffie and Martin Hellman laid the foundation for modern public key cryptography
  - DH key exchange (1976)

- Ron Rivest, Adi Shamir, and Leonard Adleman introduced the first practical implementation of public key cryptography
  - RSA algorithm (1978)

- ElGamal was introduced as an alternative of RSA (1985)

Public key cryptography

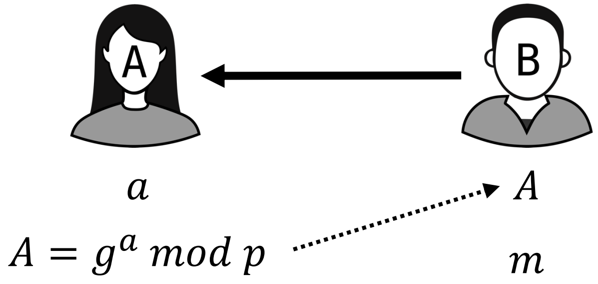
- Everybody can encrypt using the public key
  - $c = \mathrm{E}(\mathrm{k_p}, \mathrm{m})$
- Only the recipient can decrypt using the private key
  - $m = D(k_s, c)$

ElGamal encryption

- An extension of Diffie-Hellman key exchange
  - DH only provides key derivation
  - On top of that, ElGamal supports direct encryption and decryption

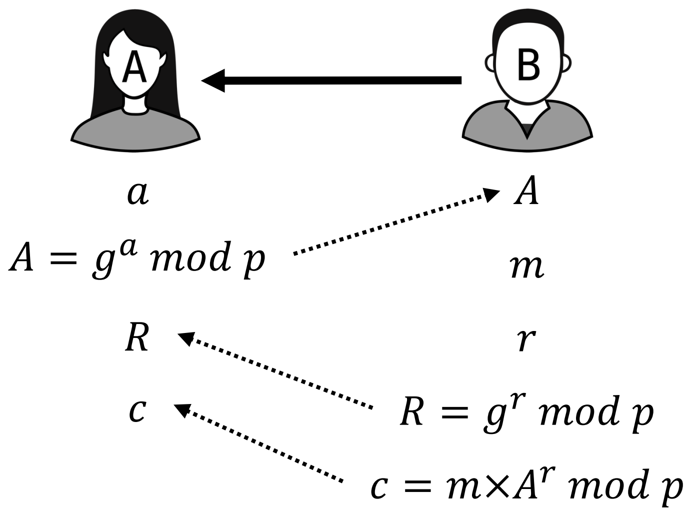
ElGamal encryption

- Alice chooses a secret key a
- Alice generates a public key $A = g^a \; mod \; p$
- Bob wants to encrypt m for Alice



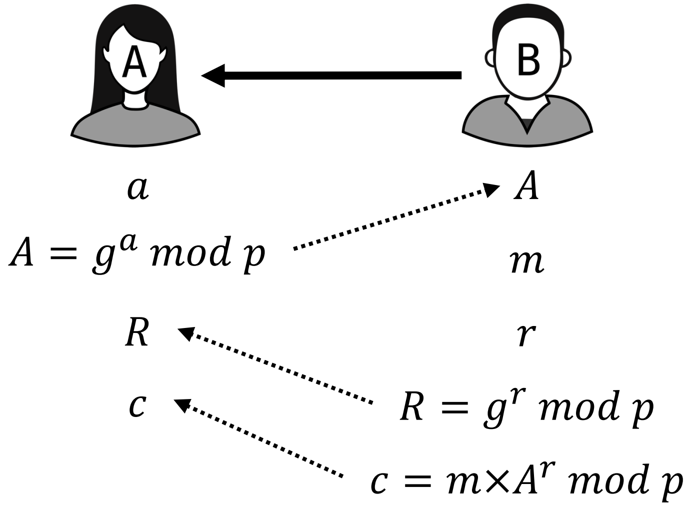
ElGamal encryption

- Alice chooses a secret key a
- Alice generates a public key $A = g^a \ mod \ p$
- Bob wants to encrypt m for Alice
  - Picks a random r and computes $R = g^r \ mod \ p$
  - Sends $\mathbf{c} = m \times A^r \ mod \ p$ and R to Alice

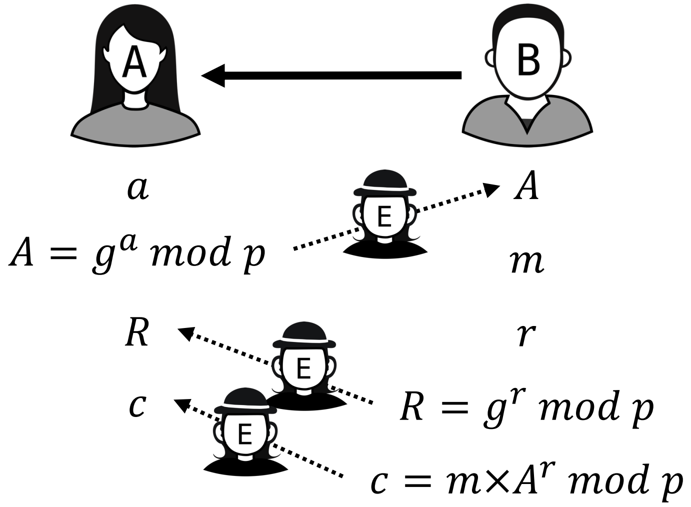


ElGamal encryption

- Alice chooses a secret key a
- Alice generates a public key $A = g^a \ mod \ p$
- Bob wants to encrypt m for Alice
  - Picks a random r and computes $R = g^r \ mod \ p$
  - Sends $\mathbf{c} = m \times A^r \ mod \ p$ and R to Alice
- Alice decrypts c by:
  - $c \times (R^a)^{-1} = m \times A^r \times R^{-a} \ mod \ p = m \times (g^a)^r \times (g^r)^{-a} \ mod \ p = m \ mod \ p$



ElGamal encryption



- Alice chooses a secret key a
- Alice generates a public key $A = g^a \, mod \, p$
- Bob wants to encrypt m for Alice
  - Picks a random r and computes $R = g^r \, mod \, p$
  - Sends $\mathbf{c} = m \times A^r \, mod \, p$ and R to Alice
- Alice decrypts c by:
  - $c \times (R^a)^{-1} = m \times A^r \times R^{-a} \, mod \, p = m \times (g^a)^r \times (g^r)^{-a} \, mod \, p = m \, mod \, p$

Security: Given A, R, and c, Eve cannot recover m

ElGamal encryption

- Example
  - Given: $p = 13$, $g = 2$
  - Alice's secret key $a = 3$
  - Alices' public key $A = g^a \; mod \; p = \; 2^3 \; mod \; 13 = 8$
  - Bob's message $m = 11$
  - Bob's random $r = 5$
  - $R = g^r \; mod \; p = 2^5 \; mod \; 13 = 6$
  - $c = m \times A^r \; mod \; p = 11 \times 8^5 \; mod \; 13 = 10$
  - Alice receives R and c from Bob
    - $m = c \times (R^a)^{-1} \; mod \; p = 10 \times 6^{-3} \; mod \; 13 = 11$

ElGamal encryption

- Example
  - Given: $p = 13$, $g = 2$
  - Alice's secret key $a = 3$
  - Alices' public key $A = g^a \ mod \ p = \ 2^3 \ mod \ 13 = 8$
  - Bob's message $m = 11$
  - Bob's random $r = 5$
  - $R = g^r \ mod \ p = 2^5 \ mod \ 13 = 6$
  - $c = m \times A^r \ mod \ p = 11 \times 8^5 \ mod \ 13 = 10$
  - Alice receives R and c from Bob
    - $m = c \times (R^a)^{-1} \ mod \ p = 10 \times 6^{-3} \ mod \ 13 = 11$ Correctly decrypted!

ElGamal encryption summary

- ElGamal encryption provides confidentiality
  - Discrete logarithm problem
- ElGamal encryption does not provide integrity
  - Mallory can tamper with the ciphertext without decrypting it
  - e.g.,
    - Mallory (MitM) receives R and c from Bob
    - Mallory sends R and $\mathrm{c}' = c \times 2$ to Alice
    - Alice decrypts c' and retrieves $m \times 2 \; mod \; 13$

Cryptography roadmap

Goal \ Scheme	Symmetric Key	Asymmetric Key
Confidentiality	✅ One Time Pad (OTP) ✅ Block ciphers (DES, AES) ✅ Stream ciphers	✅ ElGamal encryption • RSA encryption
Integrity & Authentication	• Message Authentication Code (MAC)	• Digital signature

Tools

✅ Secure key exchange

- Hash

RSA Encryption

- Idea: Prime factorization of large numbers is hard
  - Q) Prime factorize 10403

RSA Encryption

- Idea: Prime factorization of large numbers is hard
  - Q) Prime factorize 10403

```
# N = pq where p and q are primes
def factor(N):
  for i in range(2, sqrt(N)):
    if N mod i == 0:
        p = i
        q = N / i
        return (p, q)
```

This algorithm works, but takes time $O(\sqrt{N})$

e.g., using 2048 bits N, naïve factorization takes $\sqrt{2^{2048}}$

RSA Encryption

- Randomly select two large primes, p and q
- Compute public $N = pq$
- Compute $\varphi(N) = |\mathbb{Z}_N^*|$
  - If p, q are distinct primes and $N = pq$, then $\varphi(N) = (p-1)(q-1)$
- Select public key e, such that $e \in \mathbb{Z}_{\varphi(N)}^*$
  - e that is relatively prime to $(p-1)(q-1)$
- Calculate private key $d = e^{-1} \, mod \; \varphi(N)$
  - $ed = 1 \, mod \; \varphi(N)$

RSA Encryption

- $E(e, N, m) = m^e \ mod \ N = c$
- $D(d, c) = c^d \ mod \ N$

- "Magically", $m = c^d \ mod \ N$ holds
  - $c^d \ mod \ N = \ (m^e)^d \ mod \ N$
    $= m^{ed} \ mod \ N \quad \cdots ed = k\varphi(N) + 1$
    $= m^{k\varphi(N)} m^1 \ mod \ N$
    $= m \ mod \ N \quad \cdots m^{\varphi(N)} = 1 \ mod \ N$ by Euler's theorem

RSA example

- $p = 7, q = 11$
- $N = 77$
- $\varphi(N) = (p-1)(q-1) = 6 \times 10 = 60$
- Select public key e from $\mathbb{Z}_{60}^*$ → $e = 7$ (coprime to 60)
- Private key $d = e^{-1}\, mod\ \varphi(N) = 7^{-1}\, mod\ 60 = 43$
  - By the Extended Euclid's algorithm
  - Python: `pow(7, -1, 60)`

RSA example

- Given
  - Secret: $p = 7, q = 11, d = 43$
  - Public: $N = 77, e = 7$
- Plaintext $m = 8$
- Encryption
  - $c = m^e \ mod \ N = 8^7 \ mod \ 77 = 57$
- Decryption
  - $m = c^d \ mod \ N = 57^{43} \ mod \ 77 = 8$

RSA example

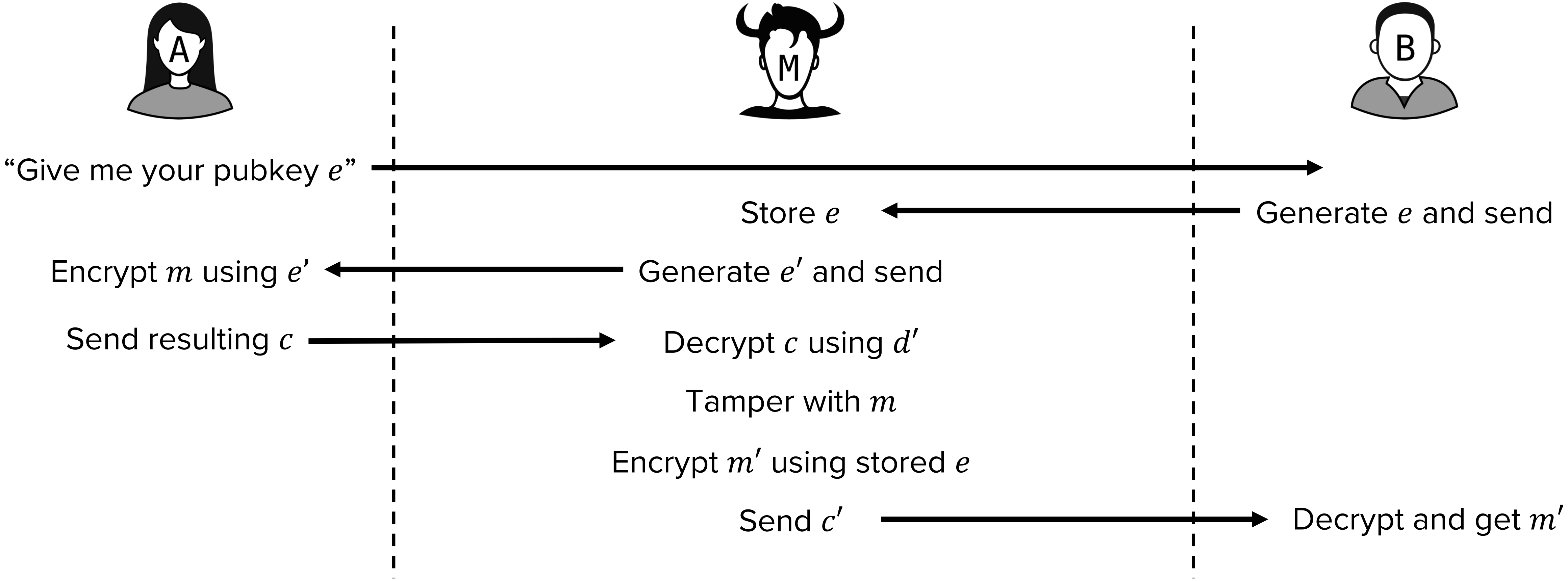
- Given
  - Secret: $p = 7, q = 11, d = 43$
  - Public: $N = 77, e = 7$
- Plaintext $m = 8$
- Encryption
  - $c = m^e \; mod \; N = 8^7 \; mod \; 77 = 57$
- Decryption
  - $m = c^d \; mod \; N = 57^{43} \; mod \; 77 = 8$ Correctly decrypted!

RSA security – confidentiality

- In order for Eve to break RSA ciphertext c given public N and public key e:
  - Need to compute $c^d \; mod \; N$
  - To compute $c^d \; mod \; N$, need to derive d
  - To derive $d = e^{-1} \; mod \; \varphi(N)$, need to find $\varphi(N)$
  - To find $\varphi(N) = (p-1)(q-1)$, need to find p and q
  - To find p and q such that $N = pq$, need to prime factorize N
  - Prime factorization is NP hard
    - No known polynomial algorithm to solve

RSA security – integrity

- RSA does not guarantee integrity
  - Susceptible to MitM attacks



Cryptography roadmap

Goal \ Scheme	Symmetric Key	Asymmetric Key
Confidentiality	✅ One Time Pad (OTP) ✅ Block ciphers (DES, AES) ✅ Stream ciphers	✅ ElGamal encryption ✅ RSA encryption
Integrity & Authentication	• Message Authentication Code (MAC)	• Digital signature

Tools

✅ Secure key exchange

- Hash

Questions?