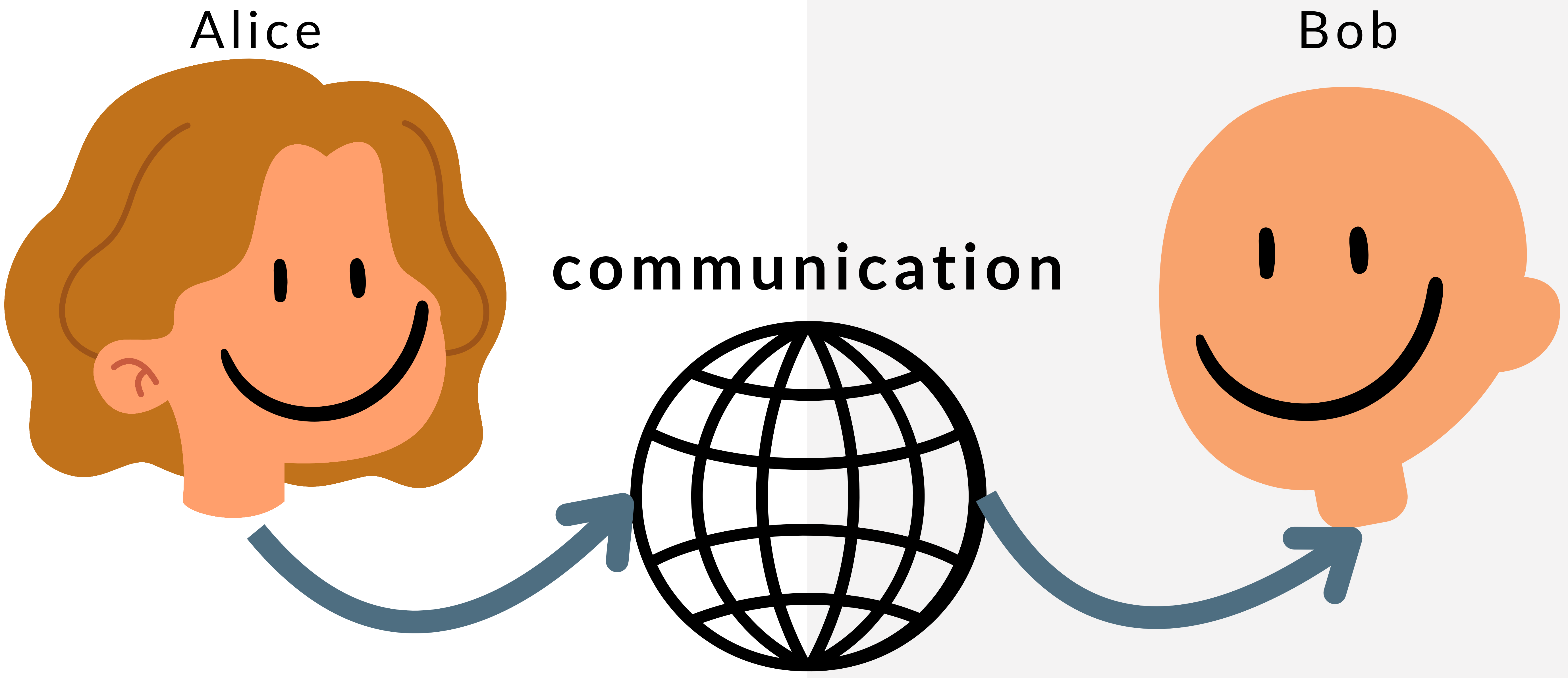
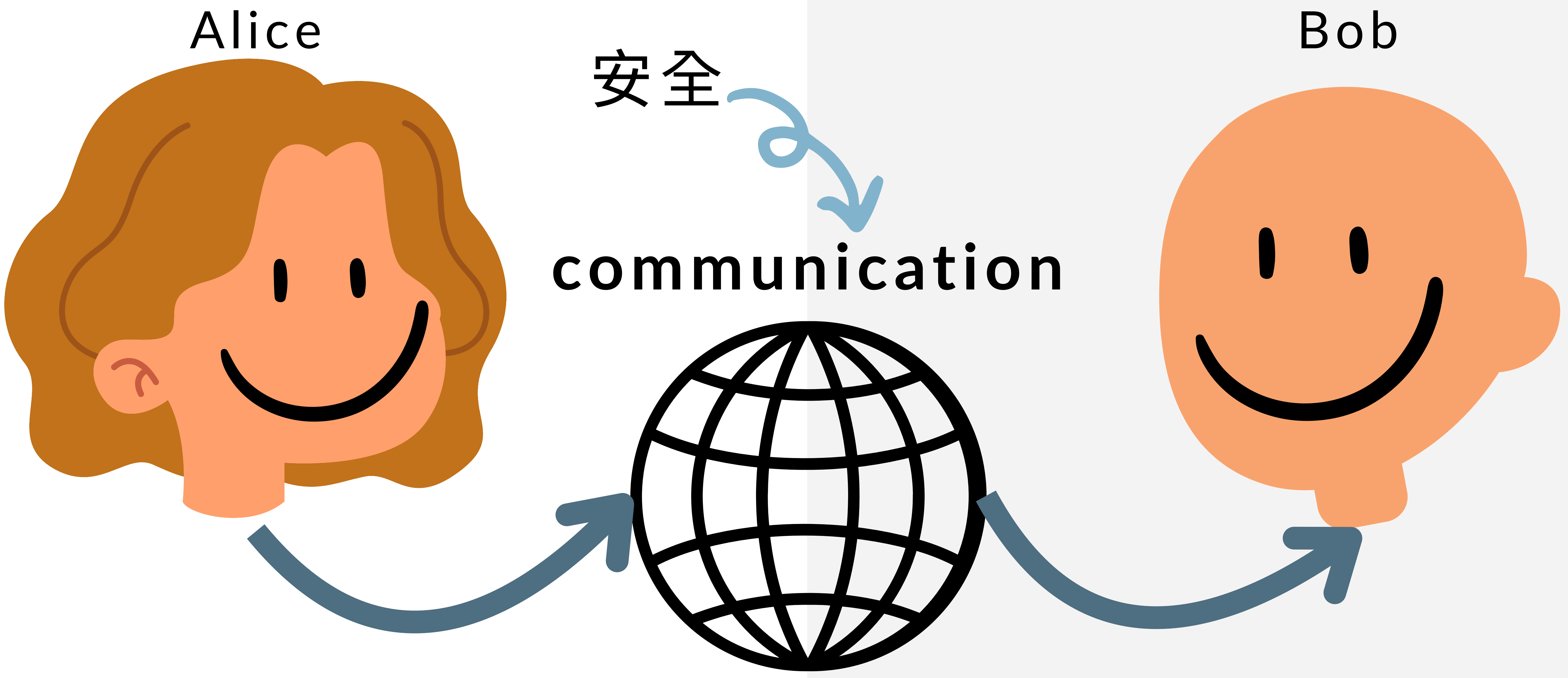
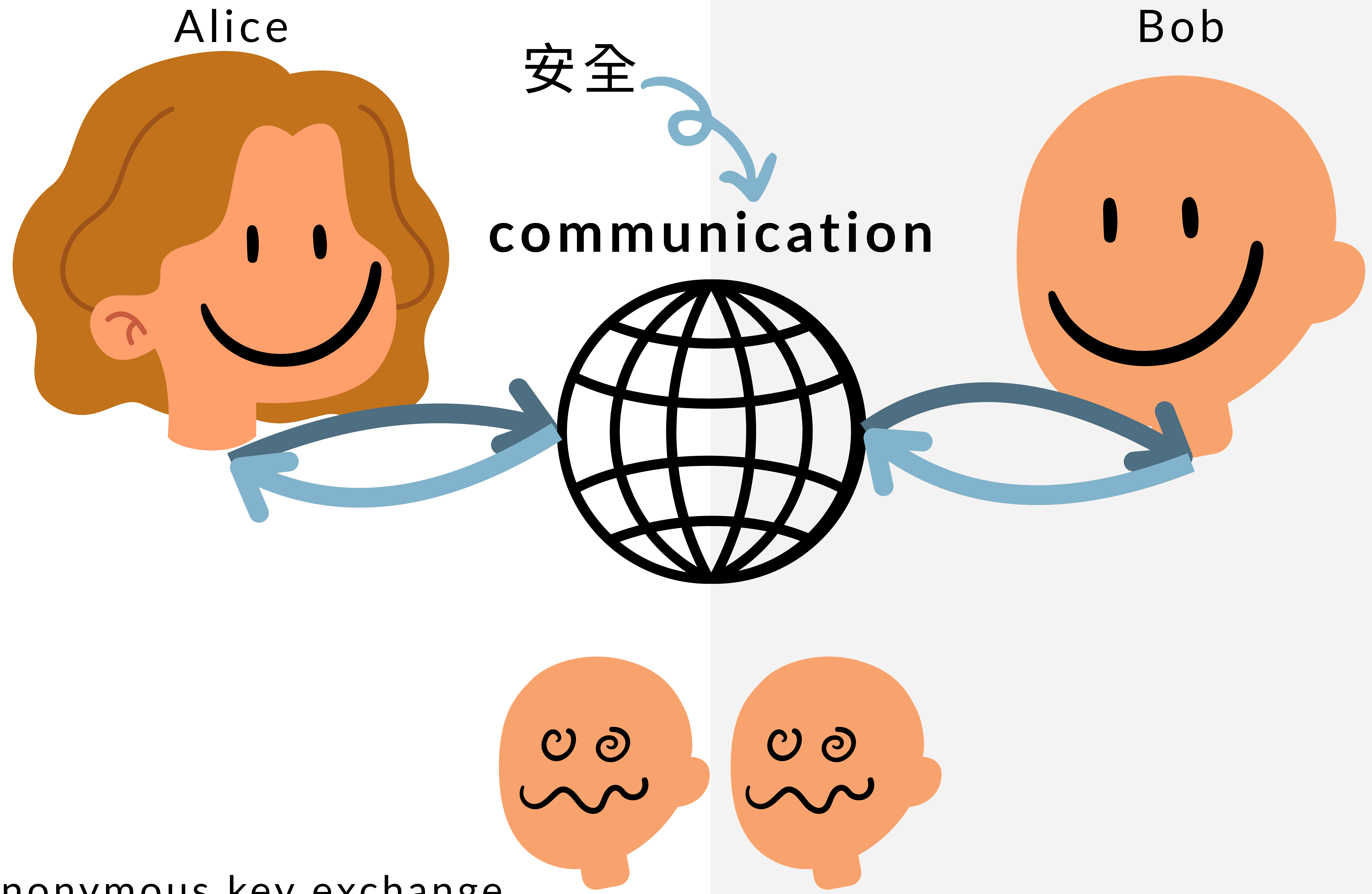
PUBLIC KEY TOOLS

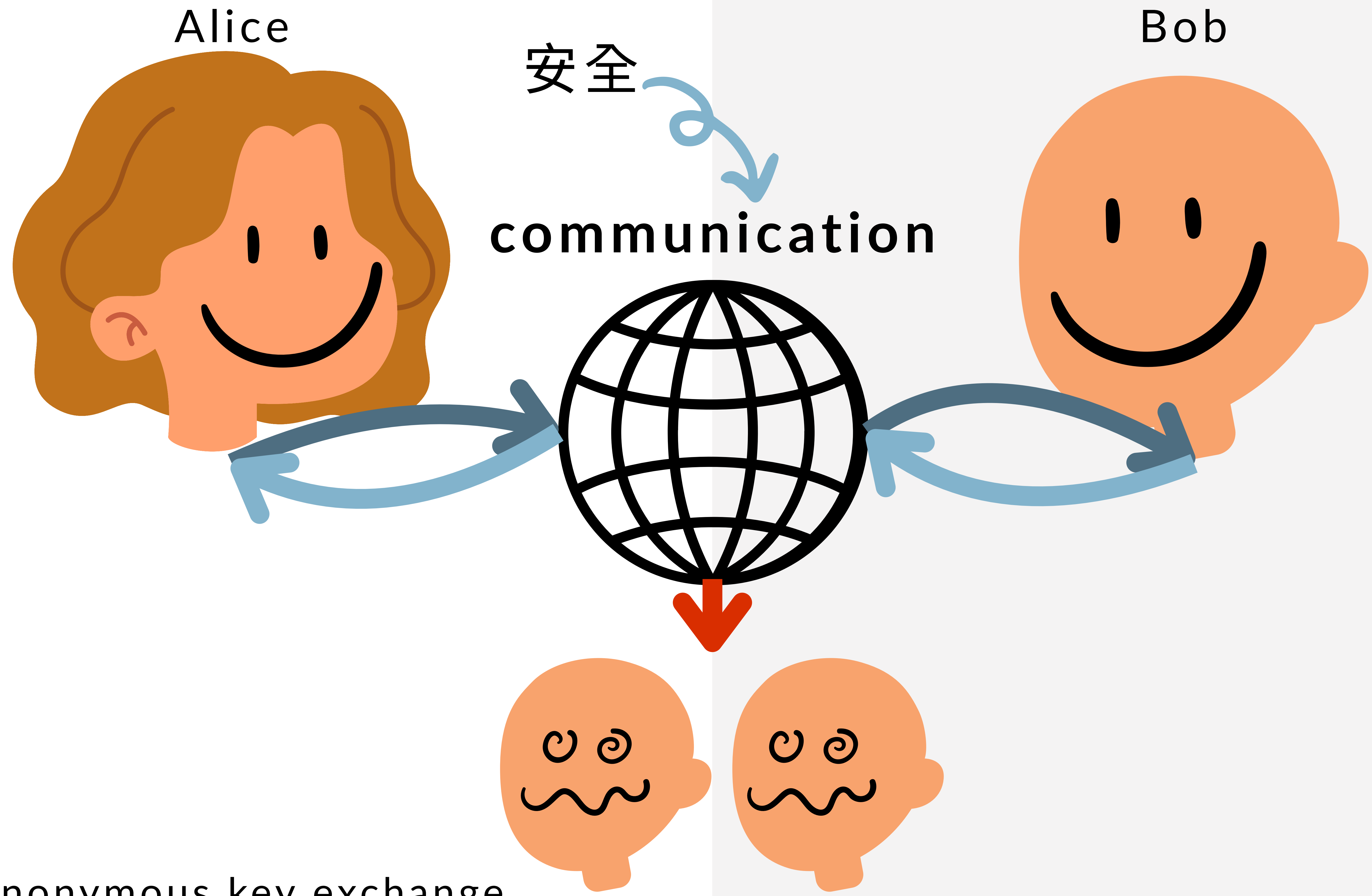
ANONYMOUS KEY EXCHANGE

匿名金鑰交換

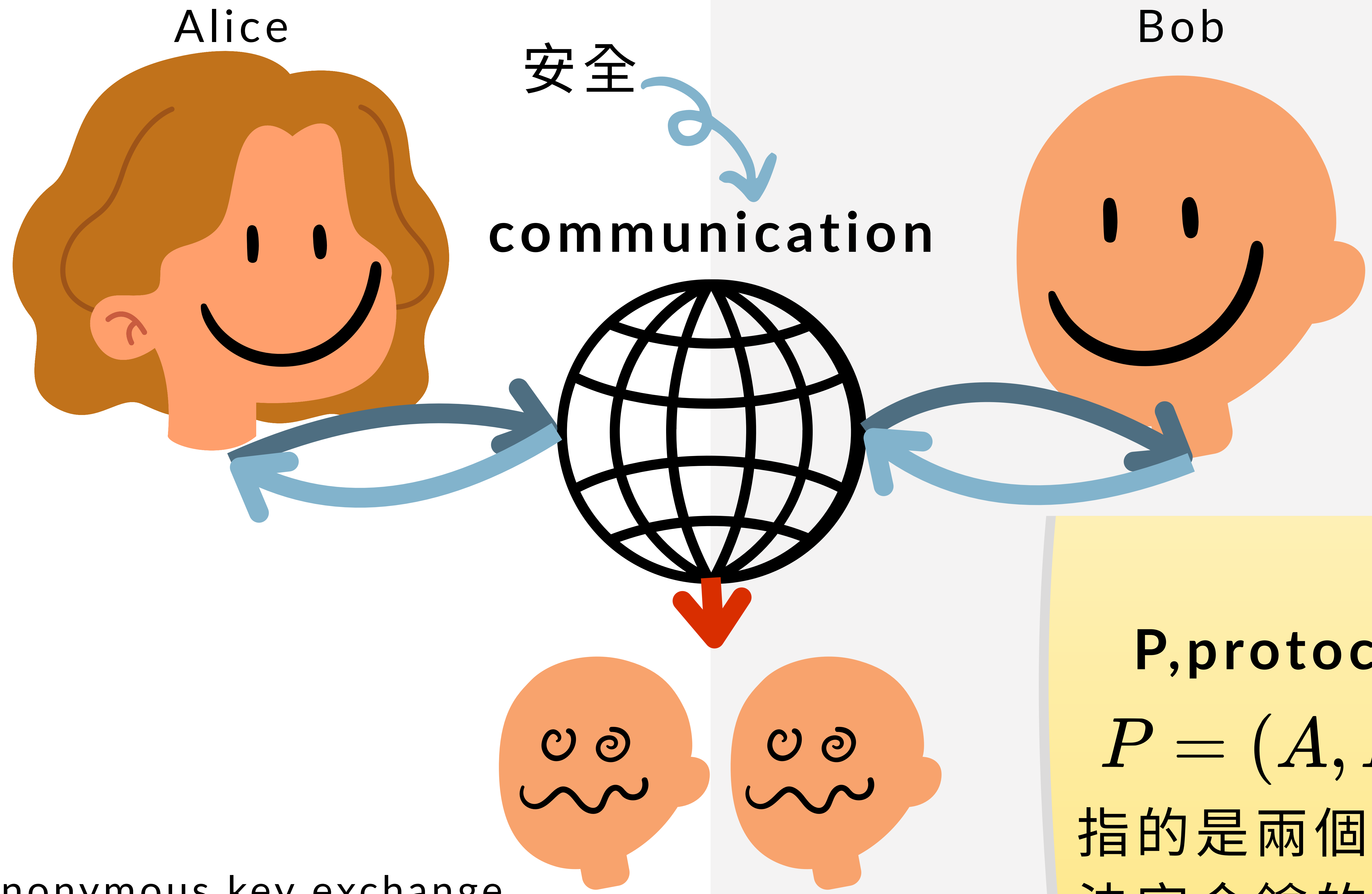

Alice
Bob
communication


Alice
安全
communication
Bob


Alice
Bob
安全
communication



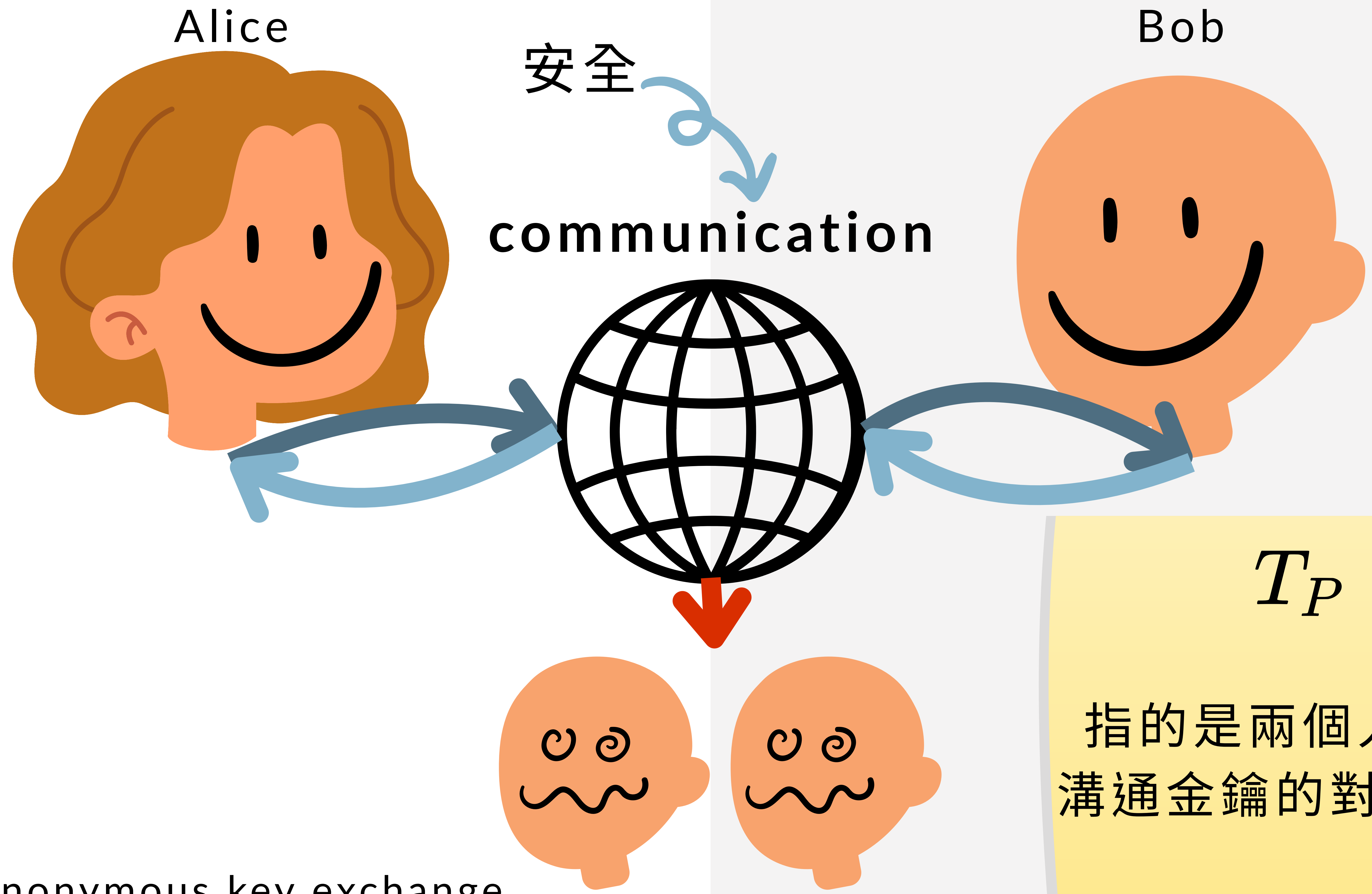
anonymous key exchange
匿名金鑰交換



P,protocol

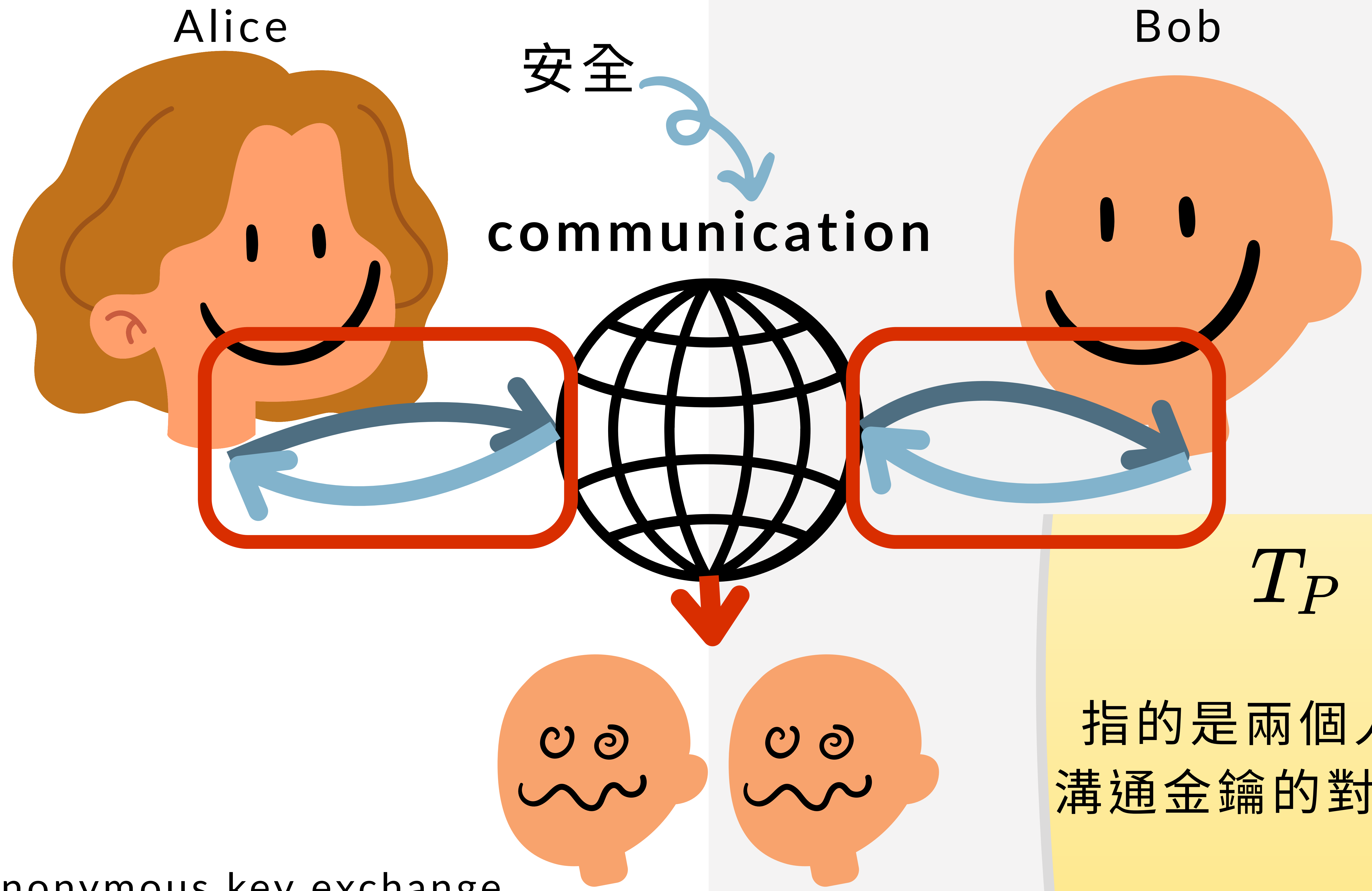
$$P = (A, B)$$

指的是兩個人之間
決定金鑰的方法



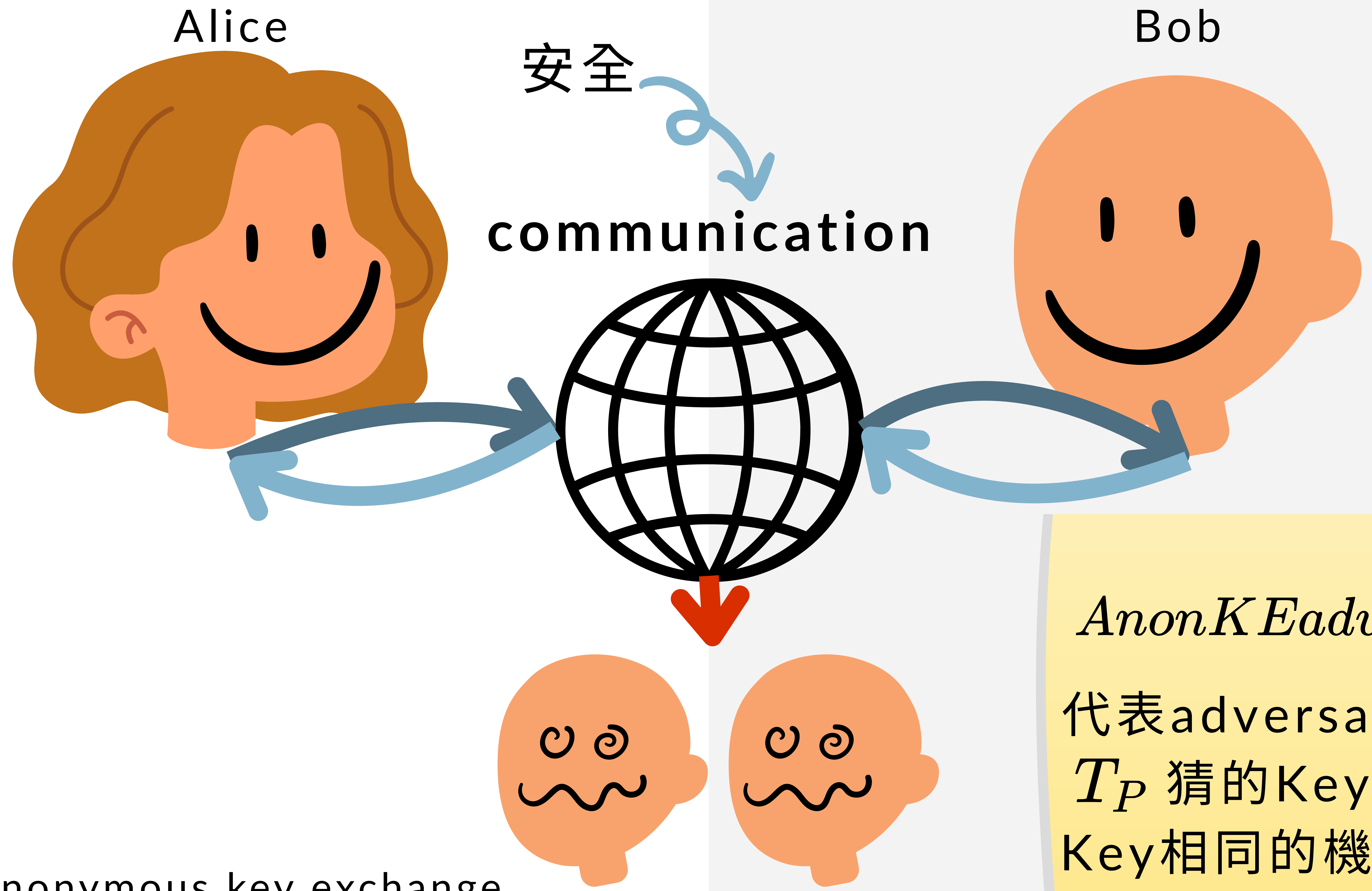
T_P

指的是兩個人之間溝通金鑰的對話紀錄



T_P

指的是兩個人之間
溝通金鑰的對話紀錄

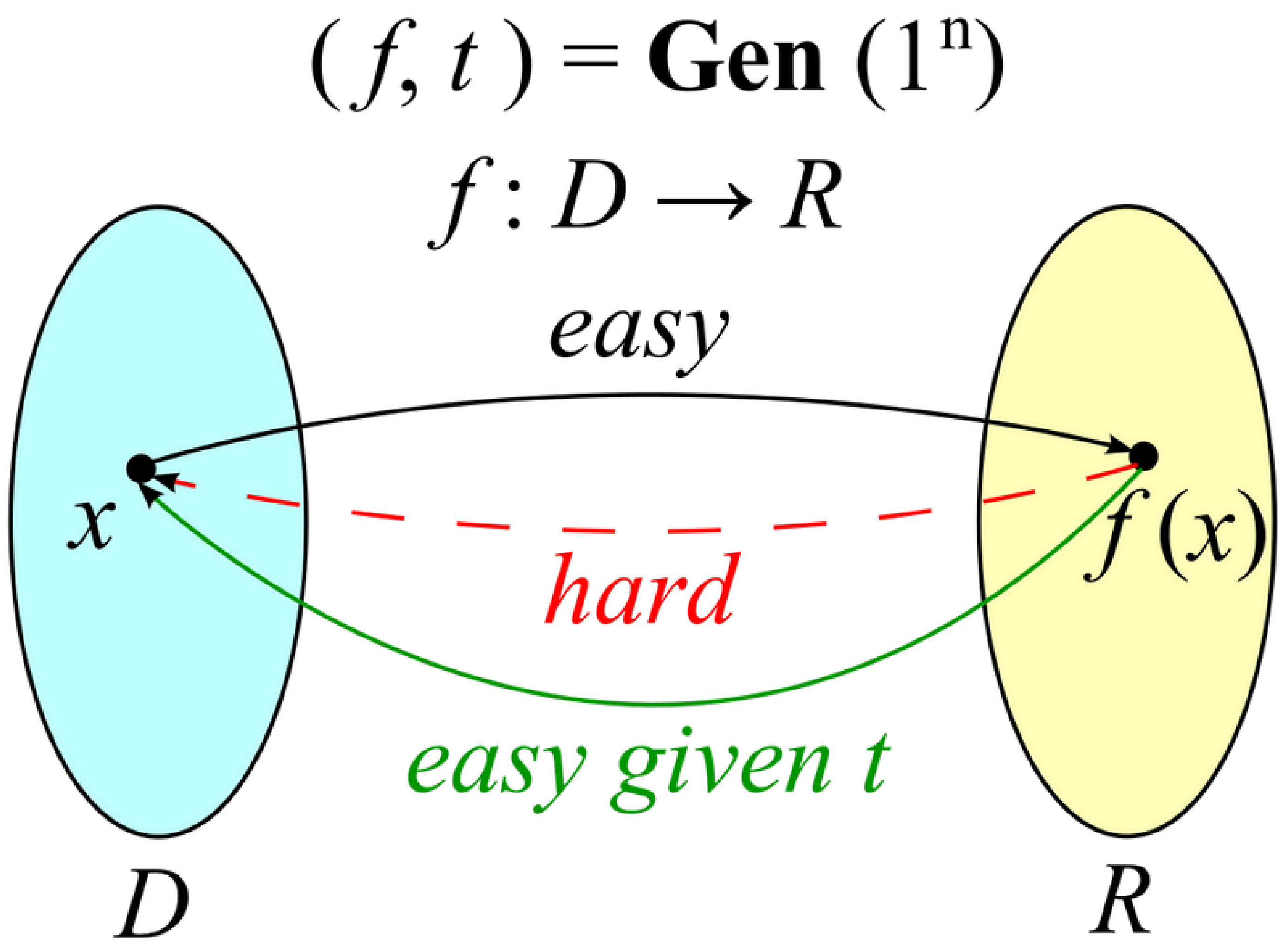


$AnonKEadv[A, P]$

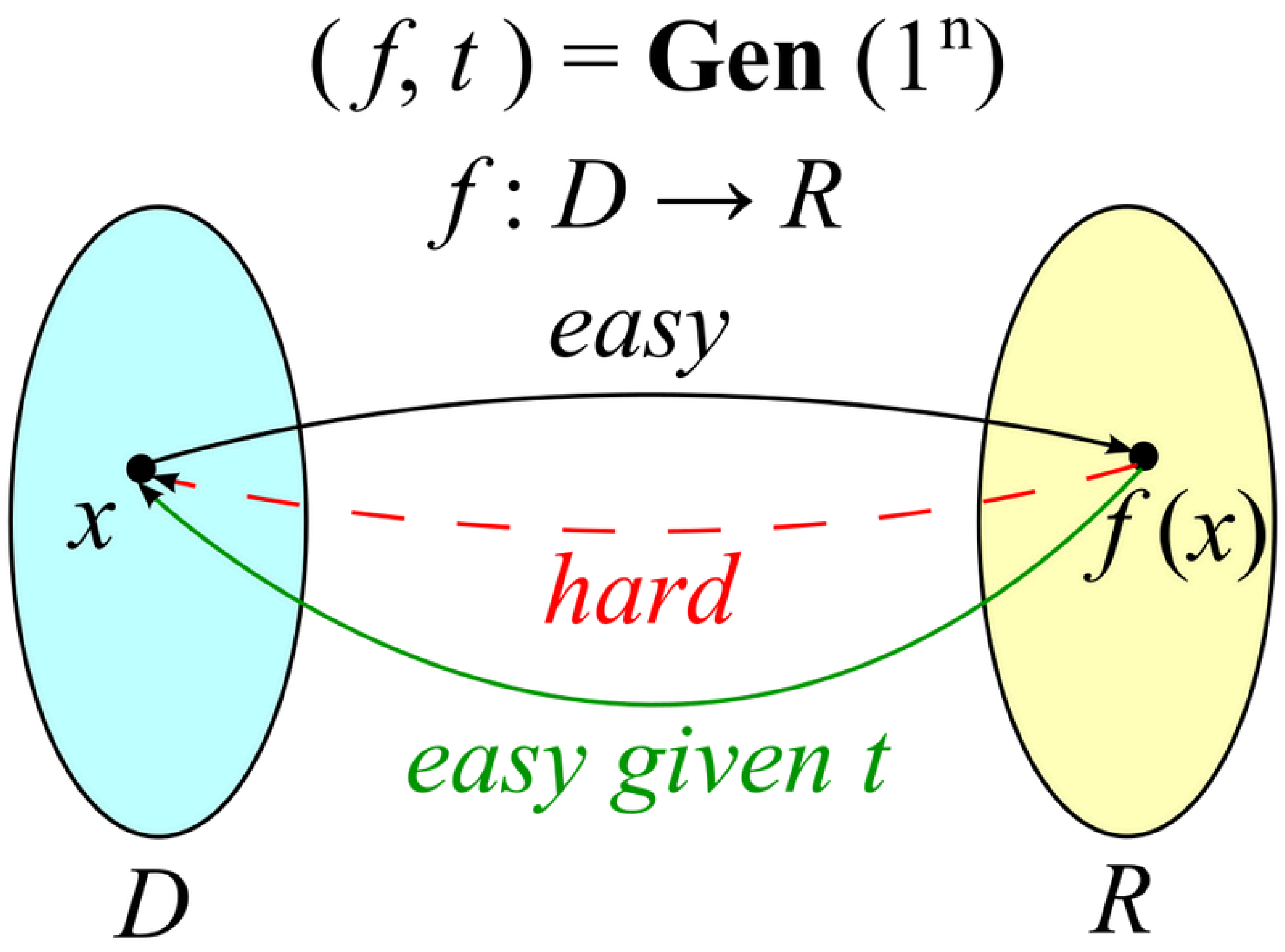
代表adversary透過 T_P 猜的Key與真實Key相同的機率

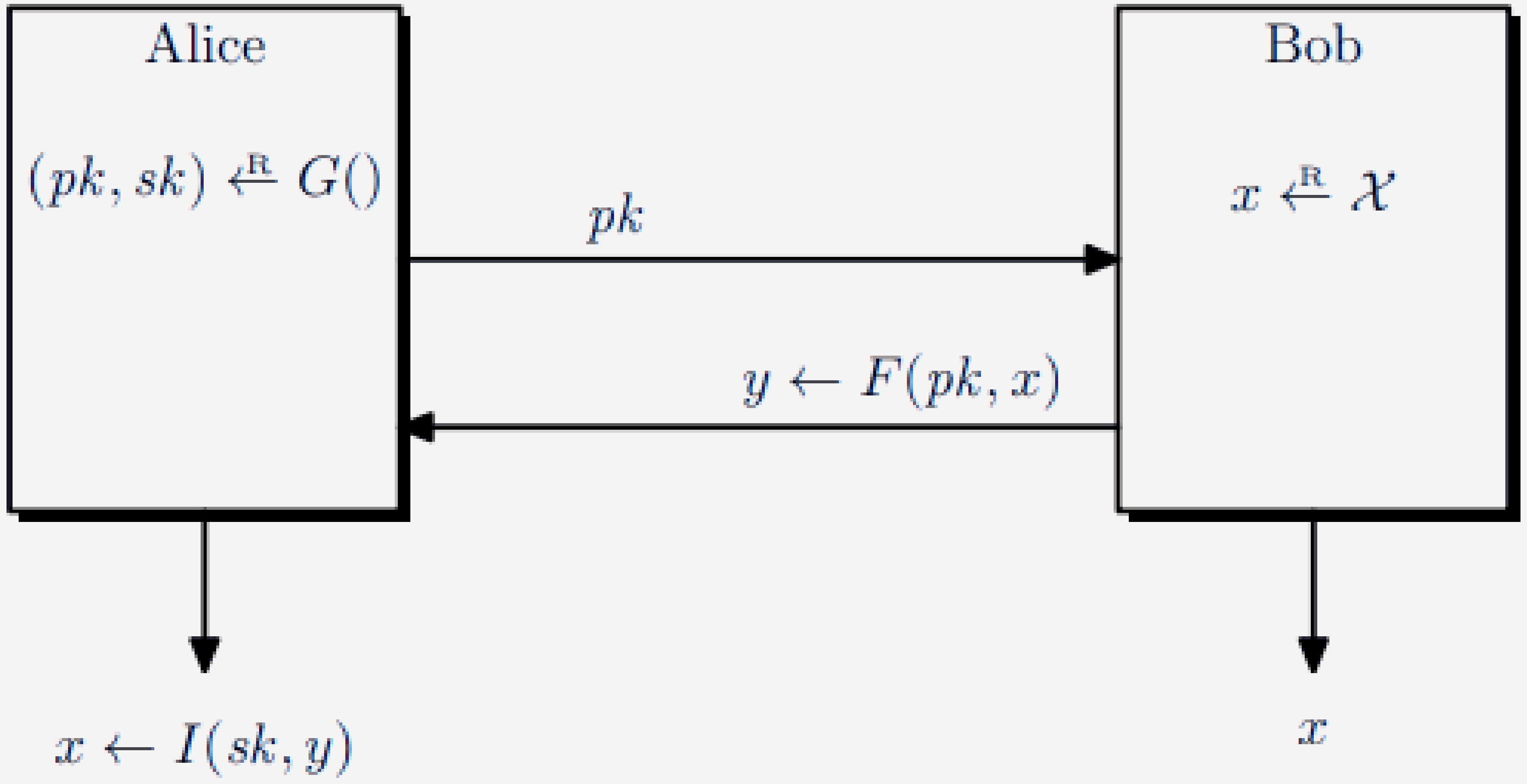
ONE-WAY TRAPDOOR FUNCTIONS

單向陷門函數

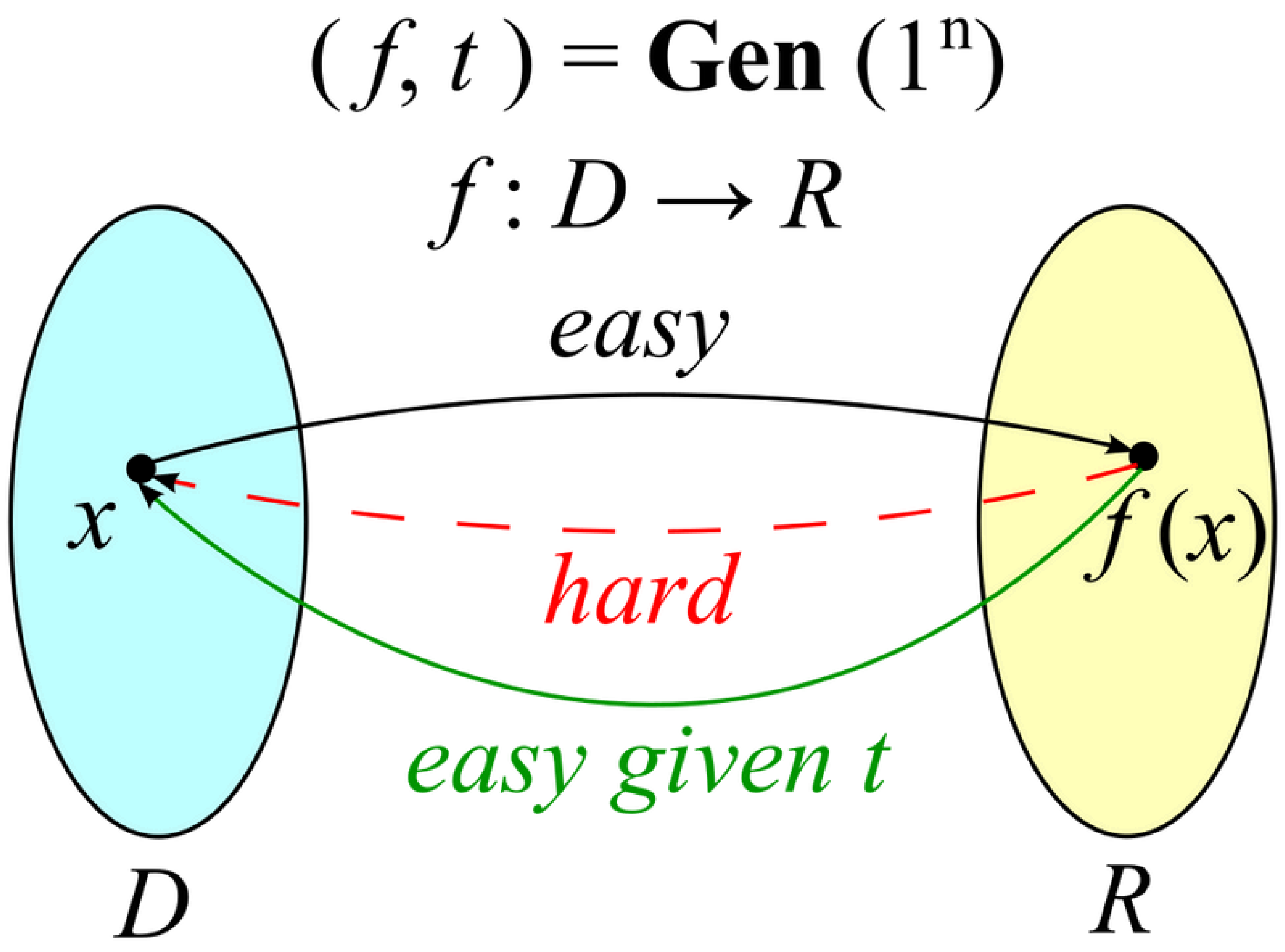


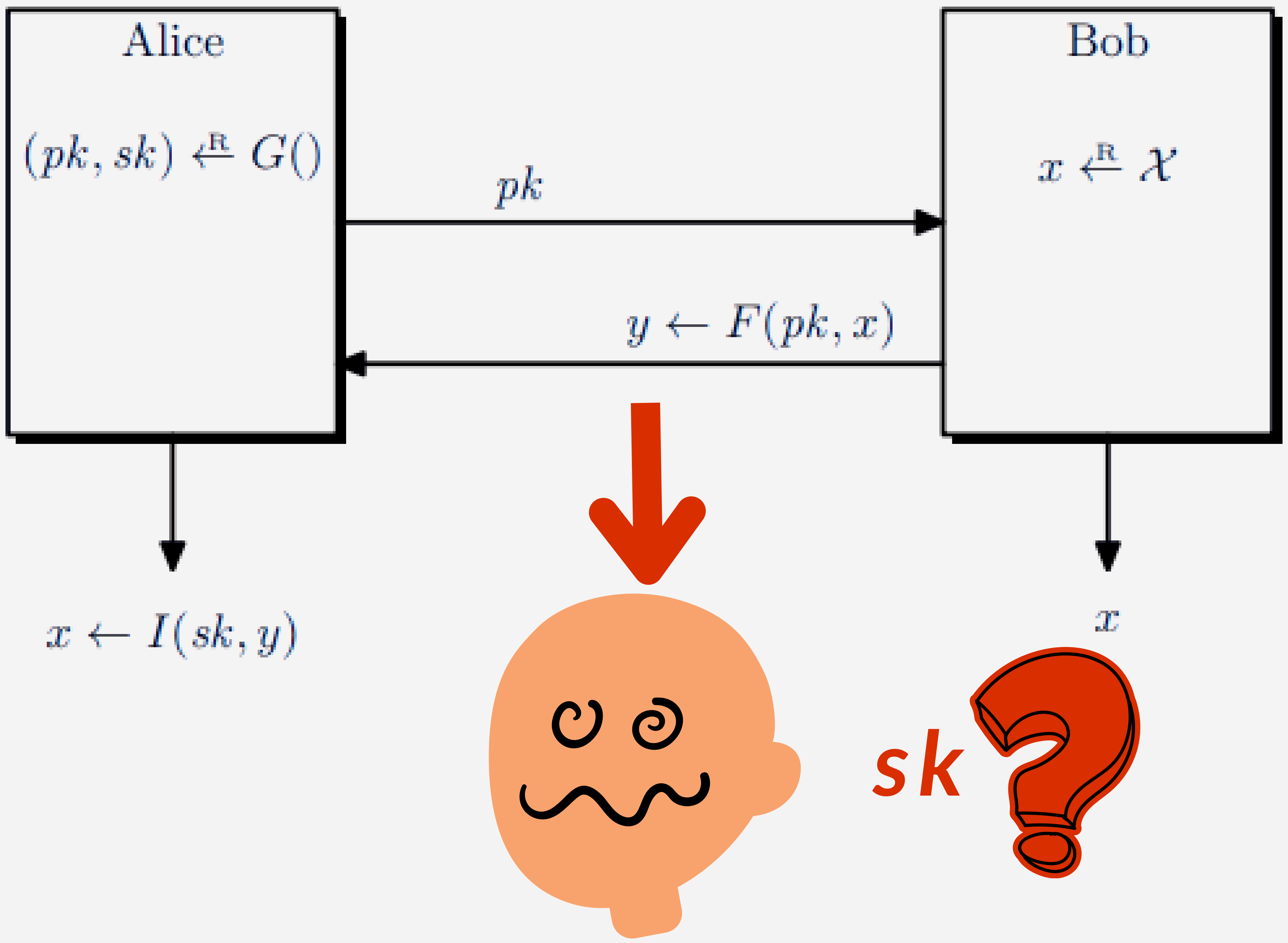
One-way trapdoor functions
單向陷門函數





One-way trapdoor functions
單向陷門函數



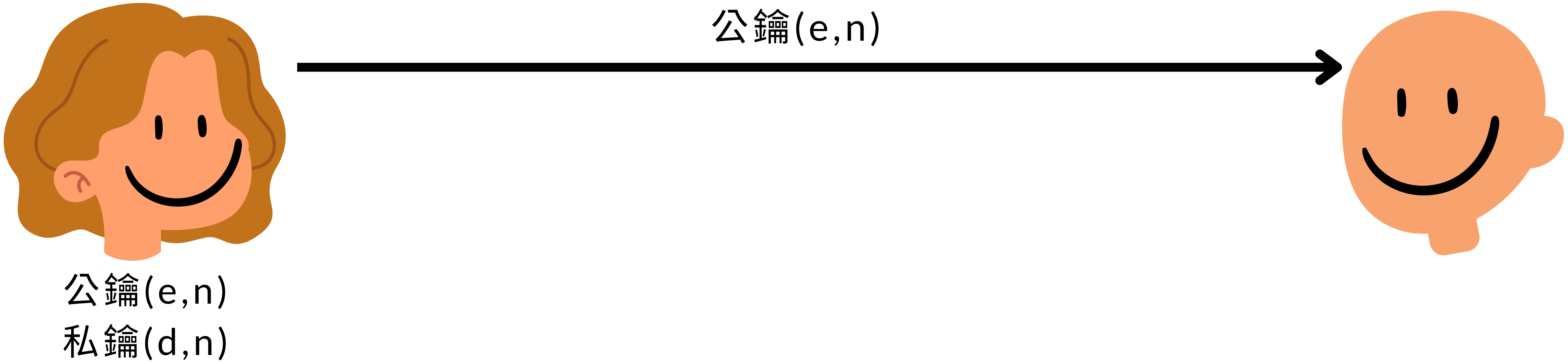


One-way trapdoor functions
單向陷門函數

A TRAPDOOR PERMUTATION SCHEME BASED ON RSA
基於RSA的陷門置換方案

RSA加密系統的安全性基於大數分解問題的困難性。其密鑰生成過程包括以下步驟：

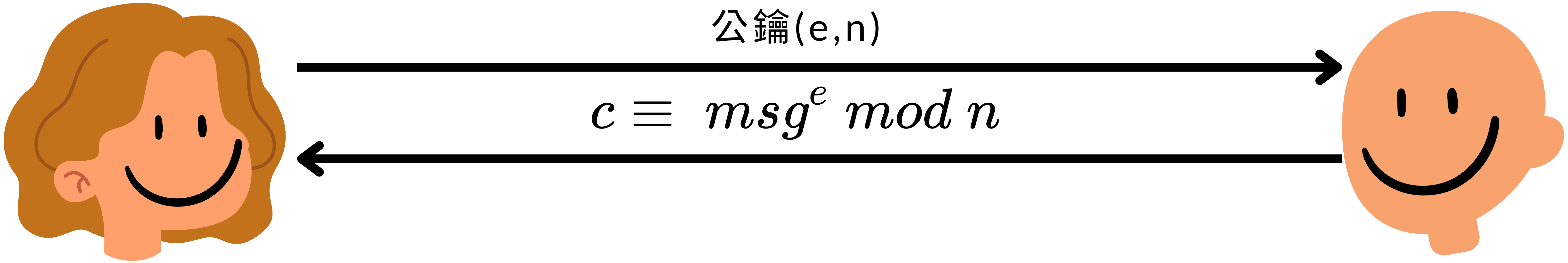
1. 選擇兩個大質數 p 和 q。
2. 計算模數 $n = p \times q, l=len(n_2)$。
3. 選擇公開指數 e。
4. 計算私鑰 d，使得 $ed\equiv 1 \bmod \Psi(n)$,其中$\Psi(n)=(q-1)(p-1)$。



基於RSA的陷門置換方案

RSA加密系統的安全性基於大數分解問題的困難性。其密鑰生成過程包括以下步驟：

1. 選擇兩個大質數 p 和 q。
2. 計算模數 n = p × q,l=len(n_2)。
3. 選擇公開指數 e。
4. 計算私鑰 d，使得 ed≡1 mod Ψ(n),其中Ψ(n)＝（q-1）（p-1)。

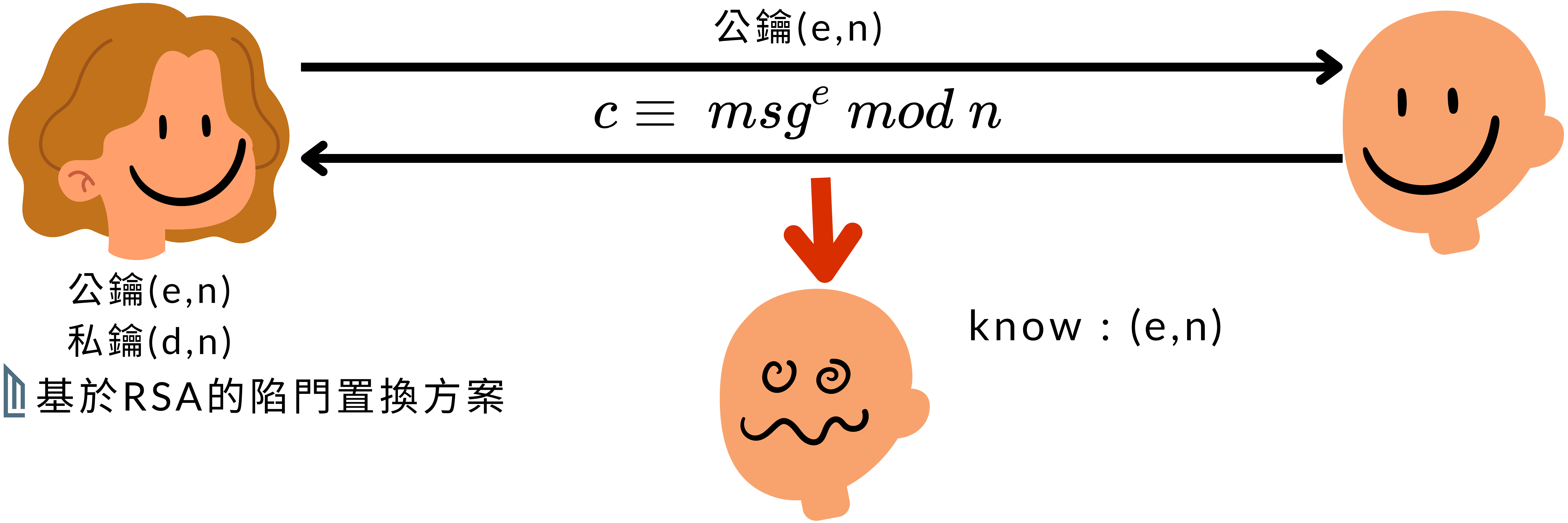


公鑰(e,n)
私鑰(d,n)

基於RSA的陷門置換方案

RSA加密系統的安全性基於大數分解問題的困難性。其密鑰生成過程包括以下步驟：

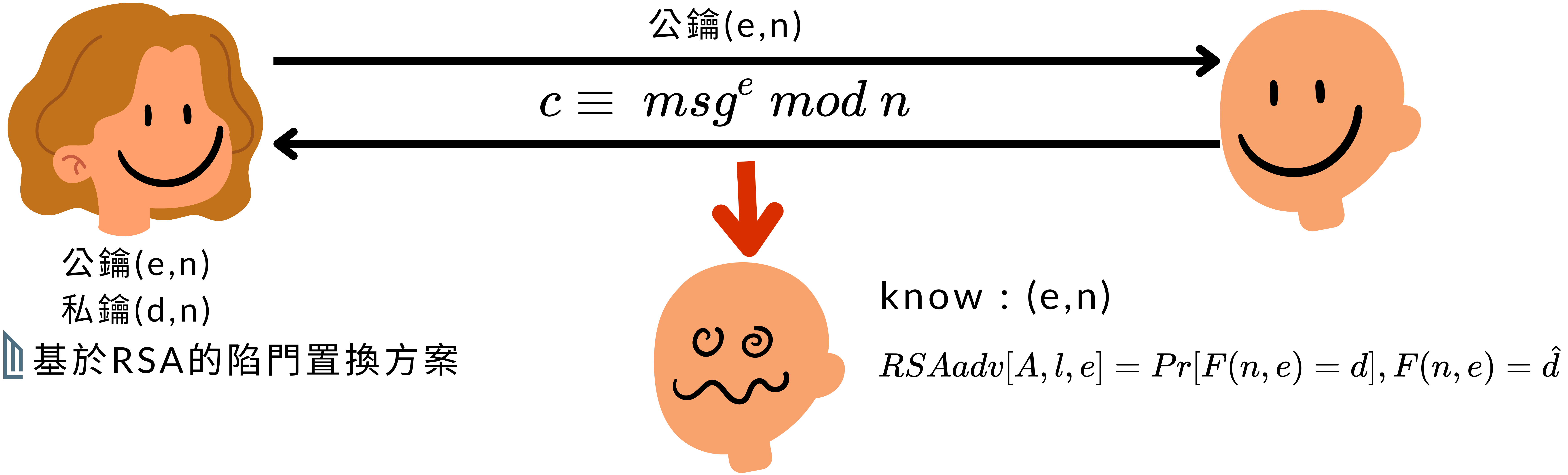
1. 選擇兩個大質數 p 和 q。
2. 計算模數 $n = p \times q, l=len(n_2)$。
3. 選擇公開指數 e。
4. 計算私鑰 d，使得 ed≡1 mod Ψ(n),其中Ψ(n)＝（q-1）（p-1)。



基於RSA的陷門置換方案

RSA加密系統的安全性基於大數分解問題的困難性。其密鑰生成過程包括以下步驟：

1. 選擇兩個大質數 p 和 q。
2. 計算模數 $n = p \times q, l=len(n_2)$。
3. 選擇公開指數 e。
4. 計算私鑰 d，使得 $ed \equiv 1 \bmod \Psi(n)$,其中$\Psi(n)$＝（q-1）（p-1)。



基於RSA的陷門置換方案

DIE-HELLMAN KEY EXCHANGE

DIE-HELLMAN密鑰交換

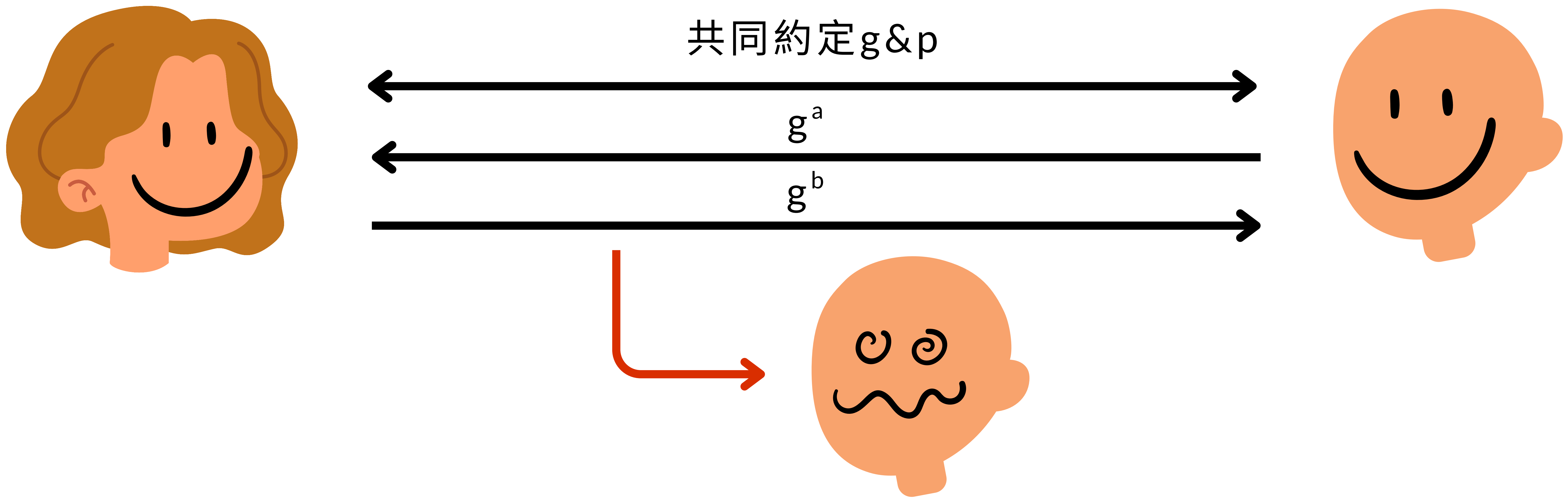
- 公開參數選定
  - 選一個大質數 p（模數）。
  - 選一個生成元 g，滿足 g<p。
  - 這兩個值 (p,g)是公開的，大家都能看到。

■

- 公開參數選定
  - 選一個大質數 p（模數）。
  - 選一個生成元 g，滿足 g<p。
  - 這兩個值 (p,g)是公開的，大家都能看到。
- 雙方產生私鑰
  - Alice 隨機挑一個私密數字 a，計算公鑰 $A=g^a \bmod p$。
  - Bob 隨機挑一個私密數字 b，計算公鑰 $B=g^b \bmod p$。
- 交換公鑰
  - Alice send A to Bob,Bob send B to Alice
  - 所有人都知道 A & B

- 公開參數選定
  - 選一個大質數 p（模數）。
  - 選一個生成元 g，滿足 g<p。
  - 這兩個值 (p,g)是公開的，大家都能看到。
- 雙方產生私鑰
  - Alice 隨機挑一個私密數字 a，計算公鑰 $A=g^a \bmod p$。
  - Bob 隨機挑一個私密數字 b，計算公鑰 $B=g^b \bmod p$。
- 交換公鑰
  - Alice send A to Bob,Bob send B to Alice
  - 所有人都知道 A & B
- 計算共享金鑰
  - $A^b = (g^a)^b = (g^b)^a = B^a$ = Secret key
- 溝通
  - Alice : $c = msg * g^{ab} \bmod p$,注意 msg < p
  - Bob：$msg = c * (g^{ab})^{-1} \bmod p$

Die-Hellman密鑰交換



- 安全性
  - adversary 知道 g, p, g^a, g^b
  - 通過 g^a 和 g^b 猜到 g^{ab} 的機率極為困難
  - 因此才有安全性(這個是 computational Die-Hellman)

假設名稱	已知條件	想要算的東西
DLP (Discrete Logarithm Problem, 離散對數問題)	g, g^a	a
CDH (Computational Diffie–Hellman, 計算型 DH)	g, g^a, g^b	g^{ab}
DDH (Decisional Diffie–Hellman, 判別型 DH)	g, g^a, g^b, g^c	判斷 $c = ab$？

DISCRETE LOGARITHM AND RELATED ASSUMPTIONS

離散對數及相關假設

- 循環群
  - 設 (G, ·) 為一個群，若存在一個元素 $g \in G$，使得 $G=\langle g \rangle=\{g^k \mid k \in Z\}$
  - G 為循環群,g 為 G 的生成元
- 離散對數假設(Discrete Logarithm Assumption, DL)
  - $G = \{ g^k \bmod q \mid k \in Z \}$,其中解是 k
  - attack game 10.4：對手猜測通過$g^k \bmod q$ 猜測出 k’
  - 而對於所有對手解決 DLP 的優勢可以忽略不計，則 DL 假設成立

- DL 假設本身不足以確保Diffie-Hellman協定的安全。DH 協定需要依賴更強的 **CDH 假設 (Computational Diffie-Hellman Assumption, CDH)**。
  - CDH 問題實例：給定 (g^{α}, g^{β})。
  - CDH 問題解：計算 $g^{\alpha\beta}$。
  - 攻擊遊戲 10.5：挑戰者計算 $u = g^{\beta}$, $v = g^{\alpha}$, $w = g^{\alpha\beta}$，並將對 (u, v) 發送給對手 A。對手 A 必須輸出 w'。
  - - 假設（定義 10.7）：如果對於所有高效能的對手 A，他們在解決 CDH 問題上的優勢（CDHadv[A,G]）可以忽略不計，則稱 CDH 假設成立。

- DDH 是一種比 CDH 更強的假設。
  - DDH 核心： DDH 假設斷言，即使是區分正確的 CDH 解與隨機群組元素，也是困難的。
  - DH-三元組：若 $\gamma=\alpha\beta$，則稱 $(g^{\alpha}, g^{\beta}, g^{\gamma})$ 為 DH-三元組。
  - 假設（定義 10.8）：DDH 假設說，沒有高效能的演算法可以有效地區分隨機 DH-三元組與隨機三元組。
  - 擊遊戲 10.6：挑戰者產生 $u = g^{\alpha}$, $v = g^{\beta}$，並隨機選擇 $b \in \{0,1\}$。若 b=0，挑戰者傳送 $w_0=g^{\alpha\beta}$; 若 b=1，傳送隨機元素 $w_1 = g^{\gamma}$。對手 A 必須輸出正確的 b 值。

COLLISION RESISTANT HASH FUNCTIONS FROM NUMBER-THEORETIC PRIMITIVES
基於數論的抗碰撞雜湊函數

基於離散對數假設的碰撞抗性雜湊函數(Collision resistance based on DL)

- 雜湊函數定義
  - $H_{DL}(\alpha,\beta)=g^{\alpha}h^{\beta}$,其中 g 為生成元、h 為隨機群元素,(α,β)為輸入參數
- 離散對數假設 (DL)
  - 給定 g,$h=g^{x}$，計算 $x=\log_{g}h$困難。
  - 攻擊者成功機率：$DLadv[B,G]=Pr[B(g,g^{x})=x]\approx 0$。
- 碰撞抗性定義 (CR)
  - 攻擊者 A 嘗試找到 (x,x′)，使得x≠x' 且 H(x)=H(x′)。
  - 成功機率：CRadv[A,H]=Pr[A 找到碰撞]。
- 由碰撞求離散對數 (Dlog)
  - $g^{\alpha}h^{\beta}=g^{\alpha'}h^{\beta'} \Rightarrow Dlog_{g}h=(\alpha-\alpha')(\beta'-\beta)$
  - $Dlog_{g}h=x$, $x=(\alpha-\alpha')(\beta'-\beta) \Rightarrow$ CRadv[A,HDL]=DLadv[B,G]。
- 結果
  - 若 DL 假設成立，則 H_{DL} 為碰撞抗性雜湊函數。

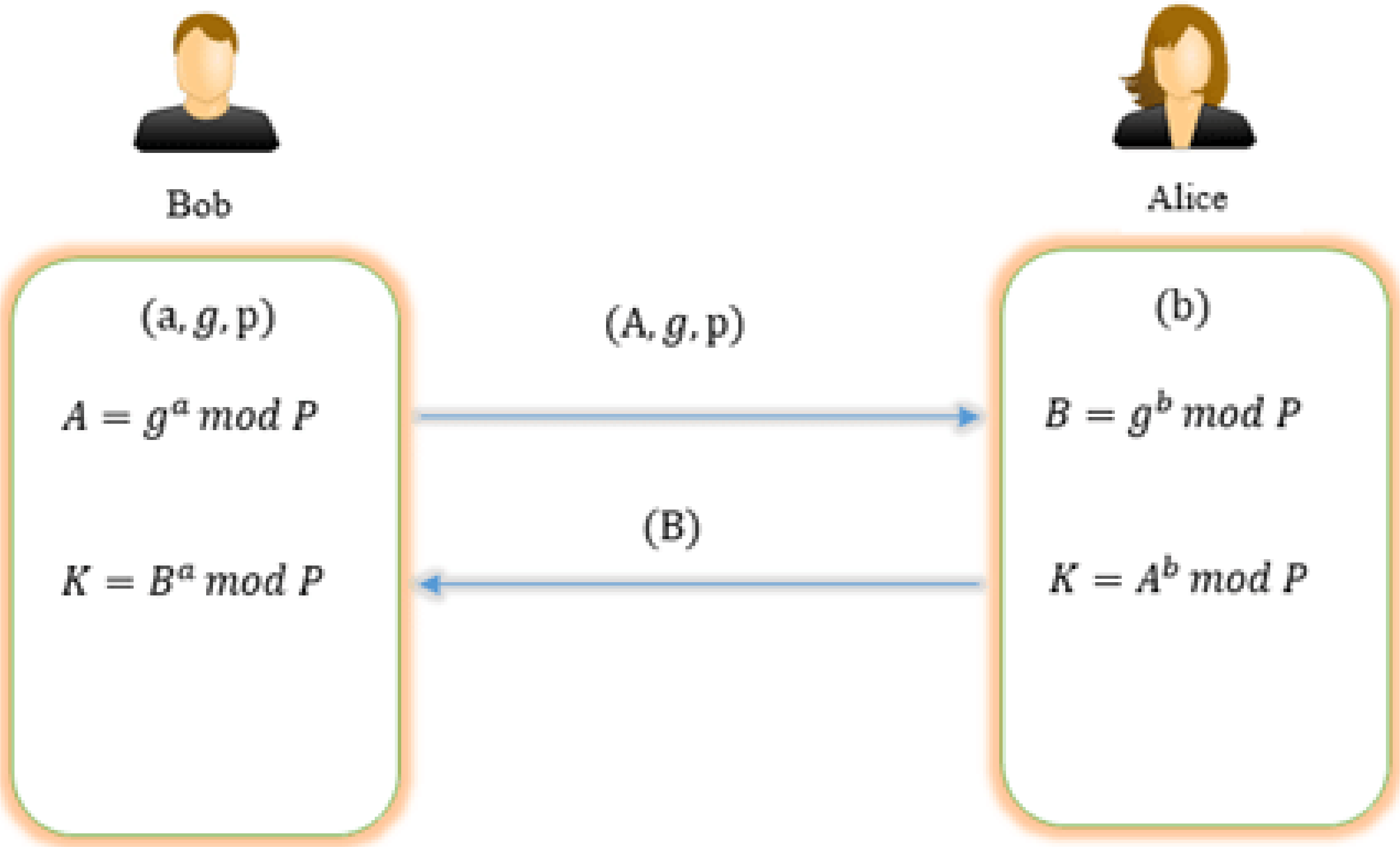
基於RSA的碰撞抗性雜湊函數(Collision resistance based on RSA)

- 雜湊函數定義
  - $H_{RSA}(x)=x^e \bmod N$,其中e 為公開指數 $N=p\times q$(兩個大質數乘積）,x 為輸入參數
- RSA假設
  - RSA 假設：給定公鑰 (N,e,y)，計算 x 使 $x^e\equiv y(\mathrm{mod} N)$很困難
  - 攻擊者成功機率：
    - $RSAadv[B,N,e]=Pr[B(N,e,y)=x]\approx 0$
- 碰撞抗性 (CR)
  - 尋找碰撞，$H_{RSA}(x)=H_{RSA}(x')\Rightarrow x^e\equiv(x')^e\ (\mathrm{mod} N)$
  - 若能找到碰撞，則可以計算出 x 的 e 次方根 → 解 RSA 問題
  - 成功機率：$CRadv[A,H_{RSA}]=Pr[A$ 找到碰撞]

基於RSA的碰撞抗性雜湊函數(Collision resistance based on RSA)

- 結果
  - $CRadv[A, H_{RSA}] = RSAadv[B, N, e]$
  - 也就是說：找到碰撞的困難度 ≈ 解 RSA 的困難度
  - 若 RSA 假設成立 → H_{RSA} 為碰撞抗性雜湊函數

ATTACKS ON THE ANONYMOUS DIE-HELLMAN PROTOCOL
對匿名 DIE-HELLMAN 協定的攻擊



- 正常的 diffe-hellman
  - Alice 選擇(p大質數,g生成元)，並計算 $A = g^a \bmod p$
  - Bob 選擇 b 並計算 $B = g^b \bmod p$
  - Alice&Bob 共同計算 $Key=B^a=A^b=g^{ab} \bmod p$

對匿名 Die-Hellman 協定的攻擊

對匿名 Diffie-Hellman 協定的中間人攻擊

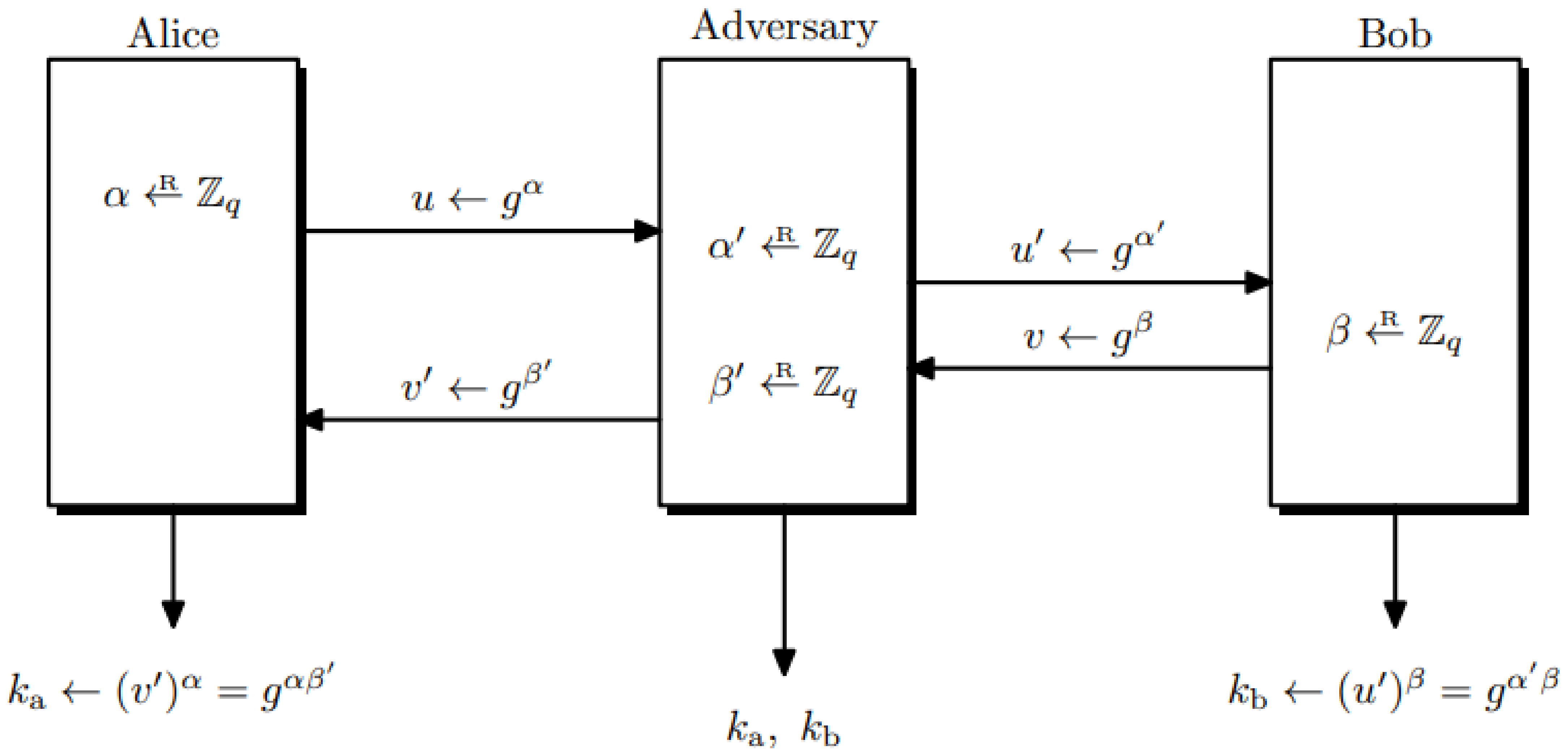


Figure 10.4: Man in the middle attack

MERKLE PUZZLES: A PARTIAL SOLUTION TO KEY EXCHANGE USING BLOCK CIPHERS MERKLE 謎題：使用分組密碼進行金鑰交換的部分解決方案

- 目的：
  - 在沒有事先共享秘密金鑰的情況下，希望雙方（Alice、Bob）能安全地建立共同金鑰。
- 核心概念：
  - 使用大量「加密謎題（encrypted puzzles）」
  - 對稱式加密（block cipher）為基礎
  - 攻擊者解題成本遠高於合法雙方

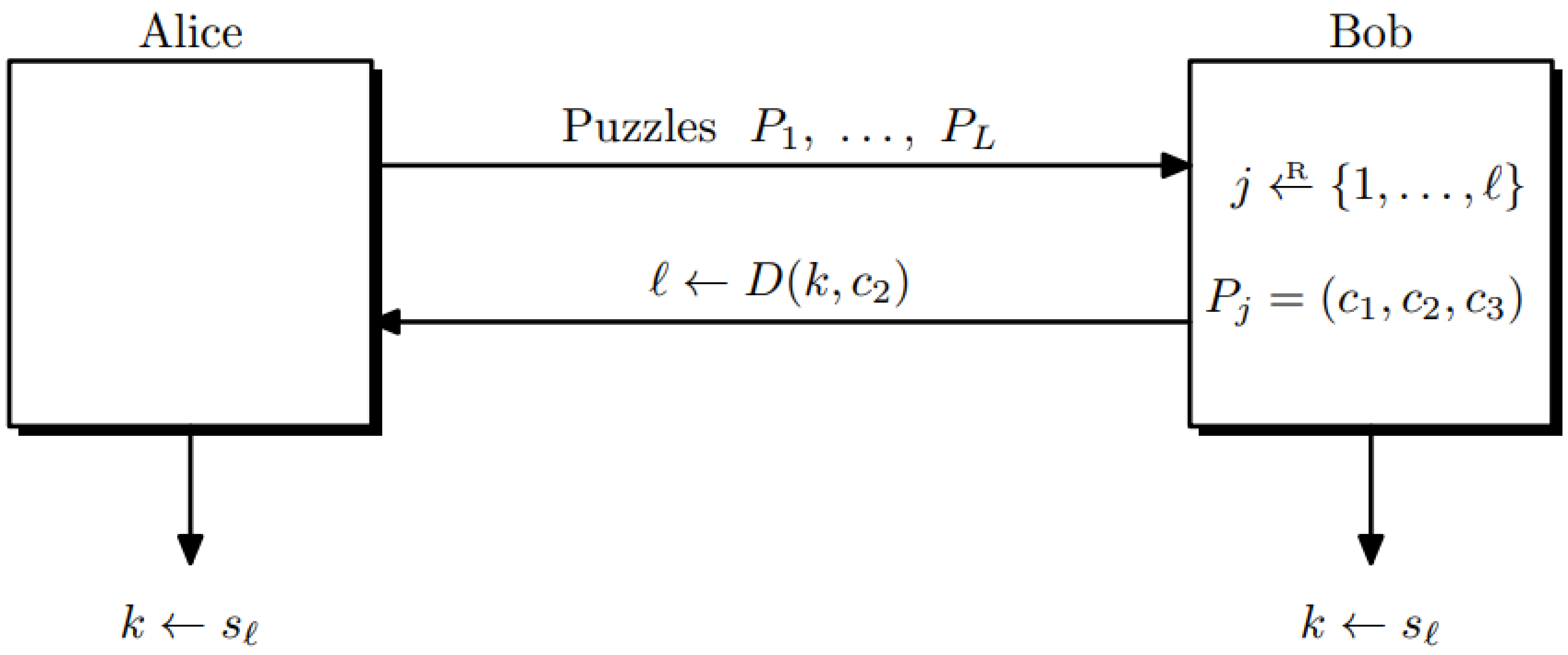


Figure 10.5: Merkle puzzles protocol

Merkle puzzles

角色	工作量	說明
Alice	O(n)	建立 n 個謎題
Bob	$O(2^k)$	解開一個謎題（平均成本）
攻擊者 Eve	$O(n \times 2^k)$	需嘗試解所有謎題

Timmerman Industries

THANK YOU

13 October, 2025