

Diffie-Hellman Key Exchange

Sicurezza informatica

v 3.3 ~ mag 2022

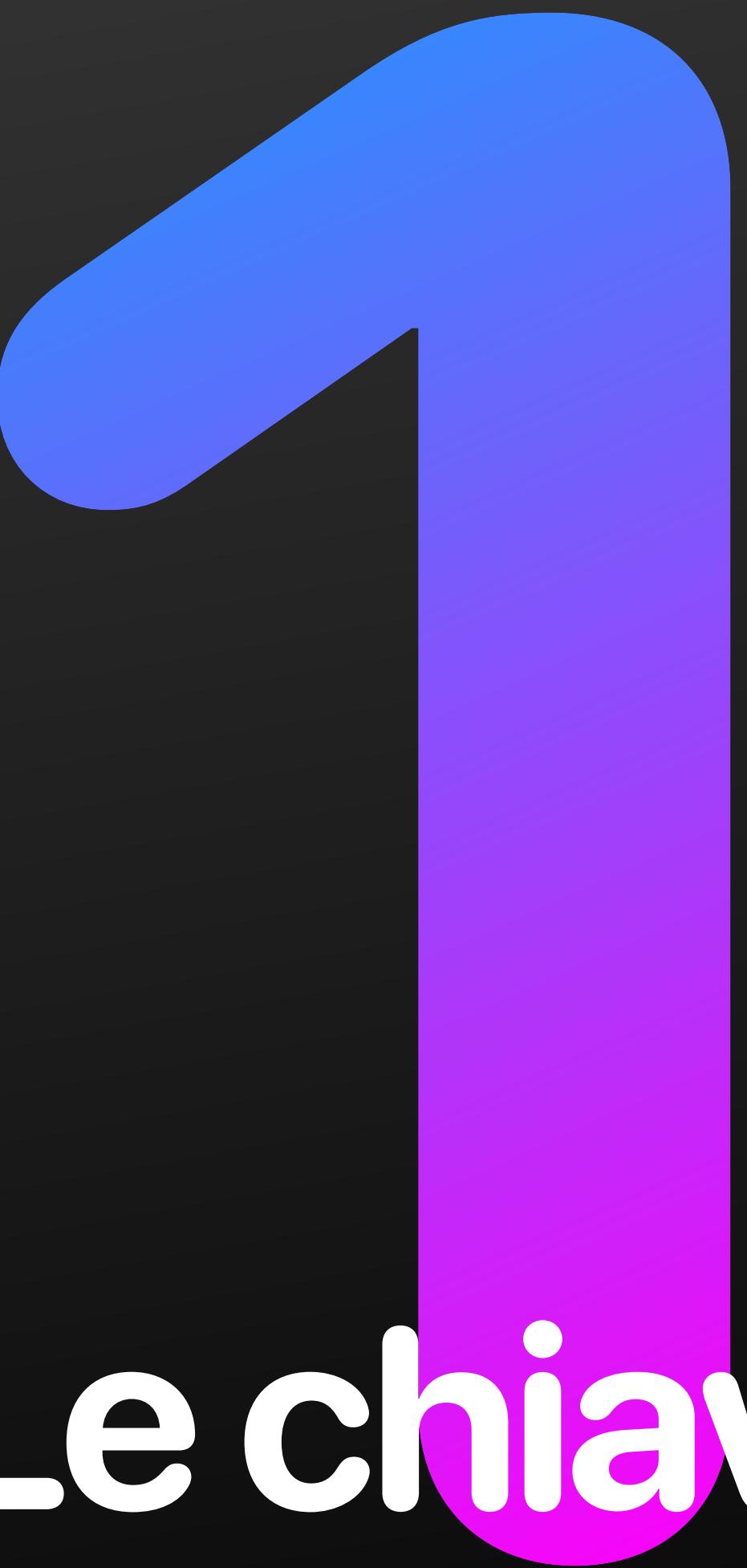


Prof. Marco Farina

marco.farina@its-ictpiemonte.it

t.me/marcofarina

in collaborazione con:



Le chiavi
crittografiche

Proprietà delle chiavi crittografiche



Casuale



Protetta



Condivisa

La potenza di un sistema crittografico dipende dalla tecnica usata per condividere la chiave.

Come si può condividere la chiave?



A mano



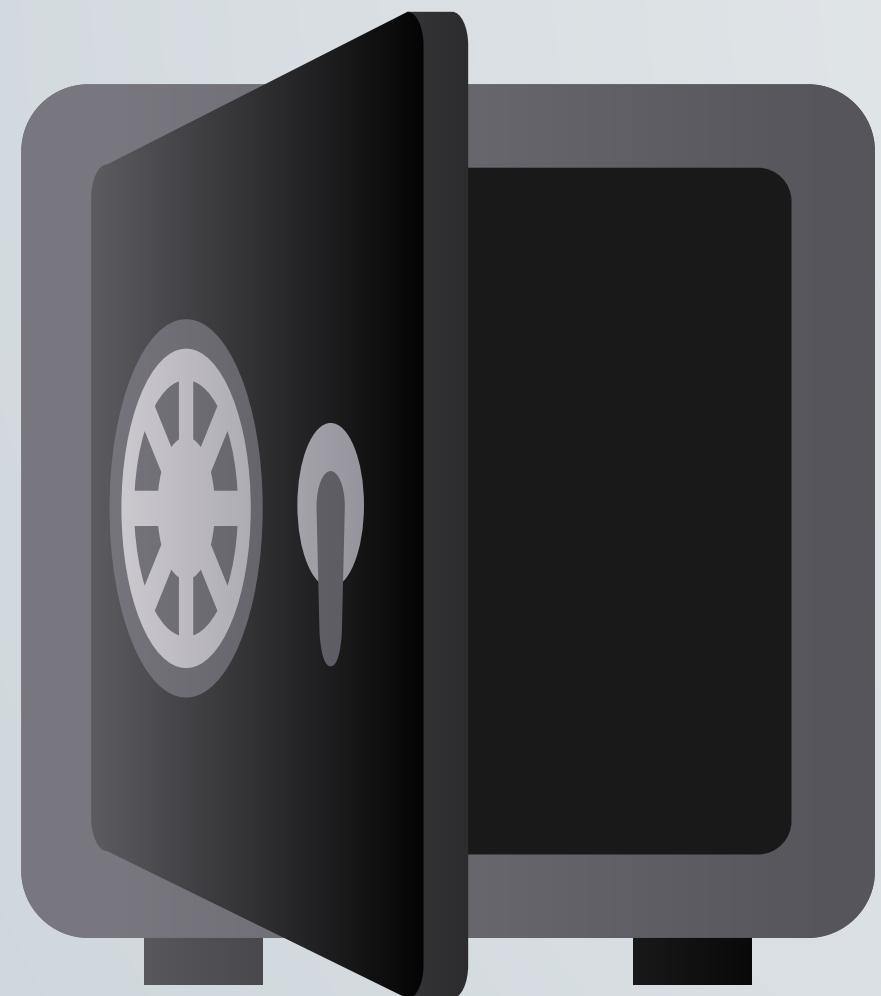
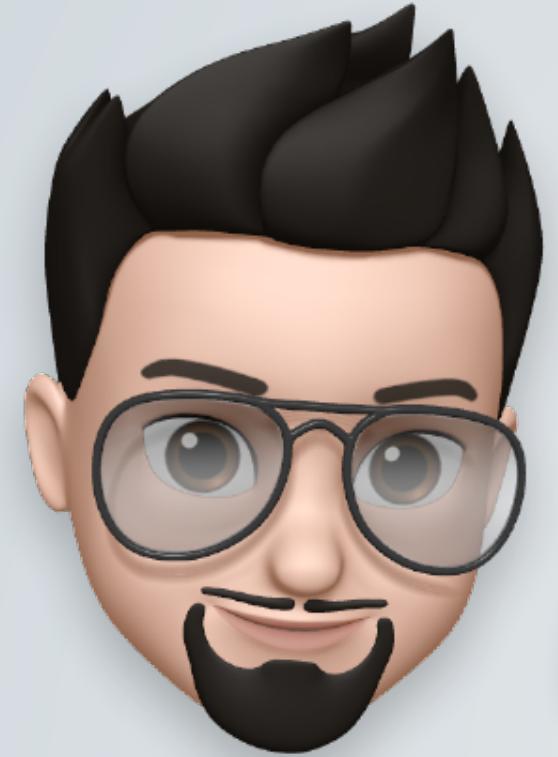
Terza parte



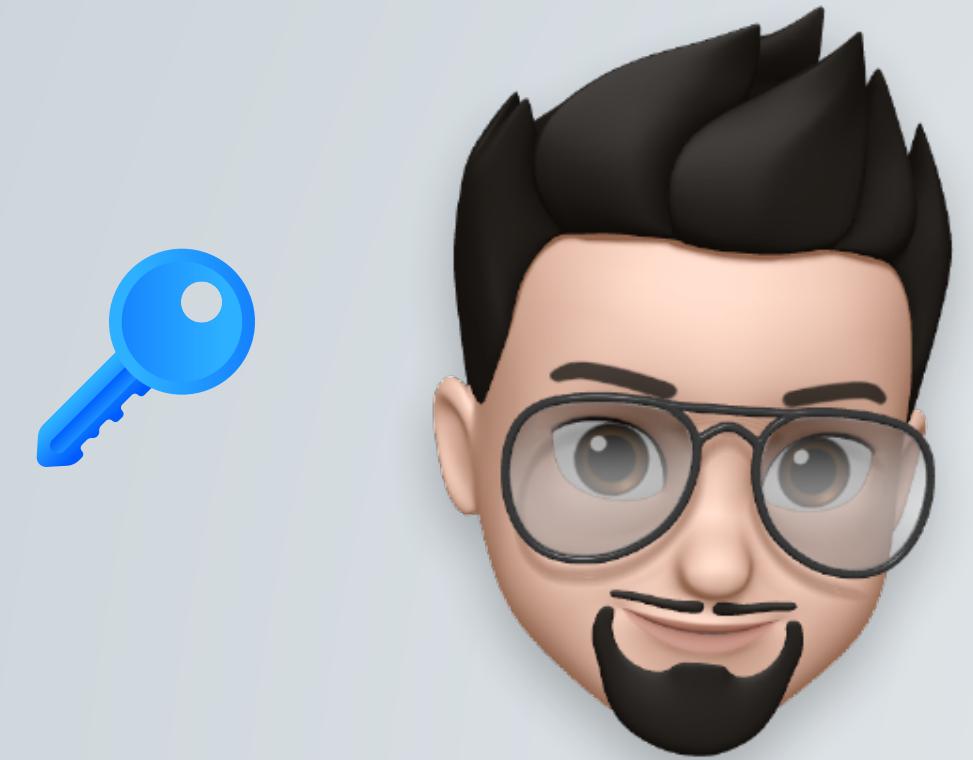
Canale sicuro

I primi due metodi non sono utilizzabili in epoca informatica; il terzo presuppone che una chiave sia già stata scambiata.

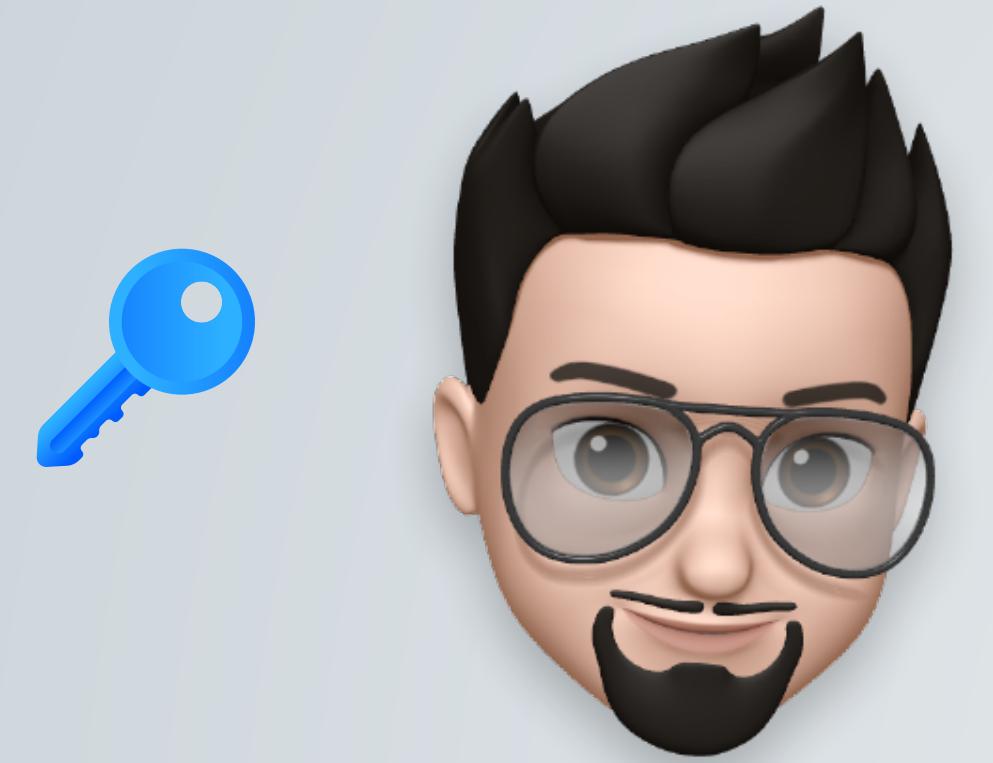
Il metodo dei lucchetti



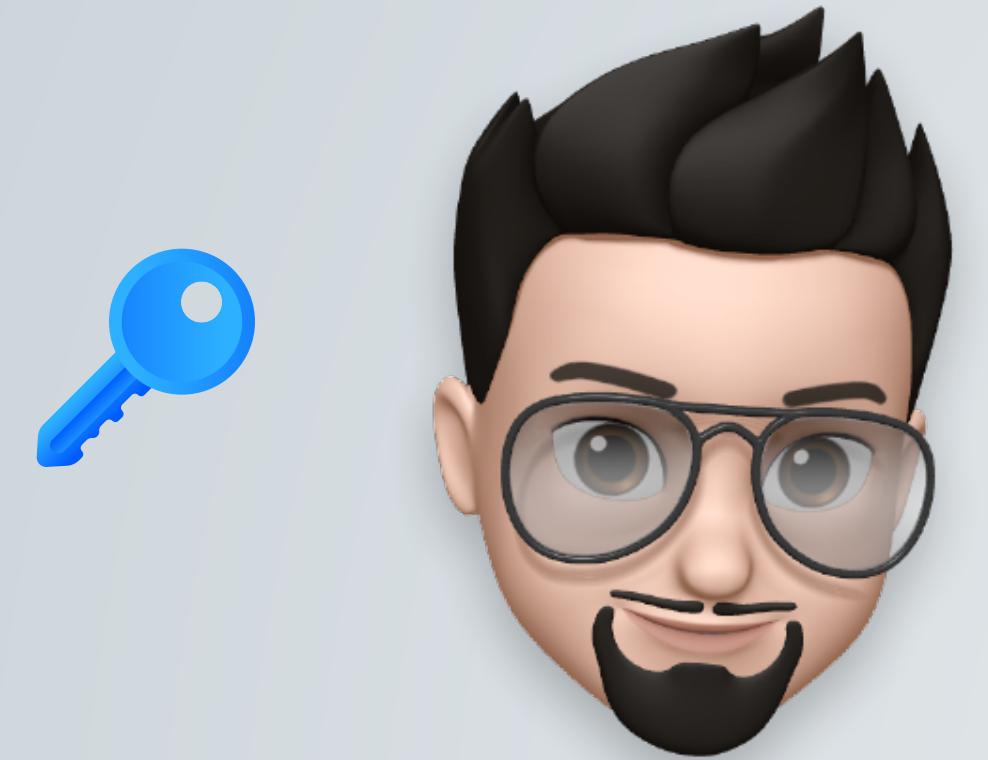
Il metodo dei lucchetti



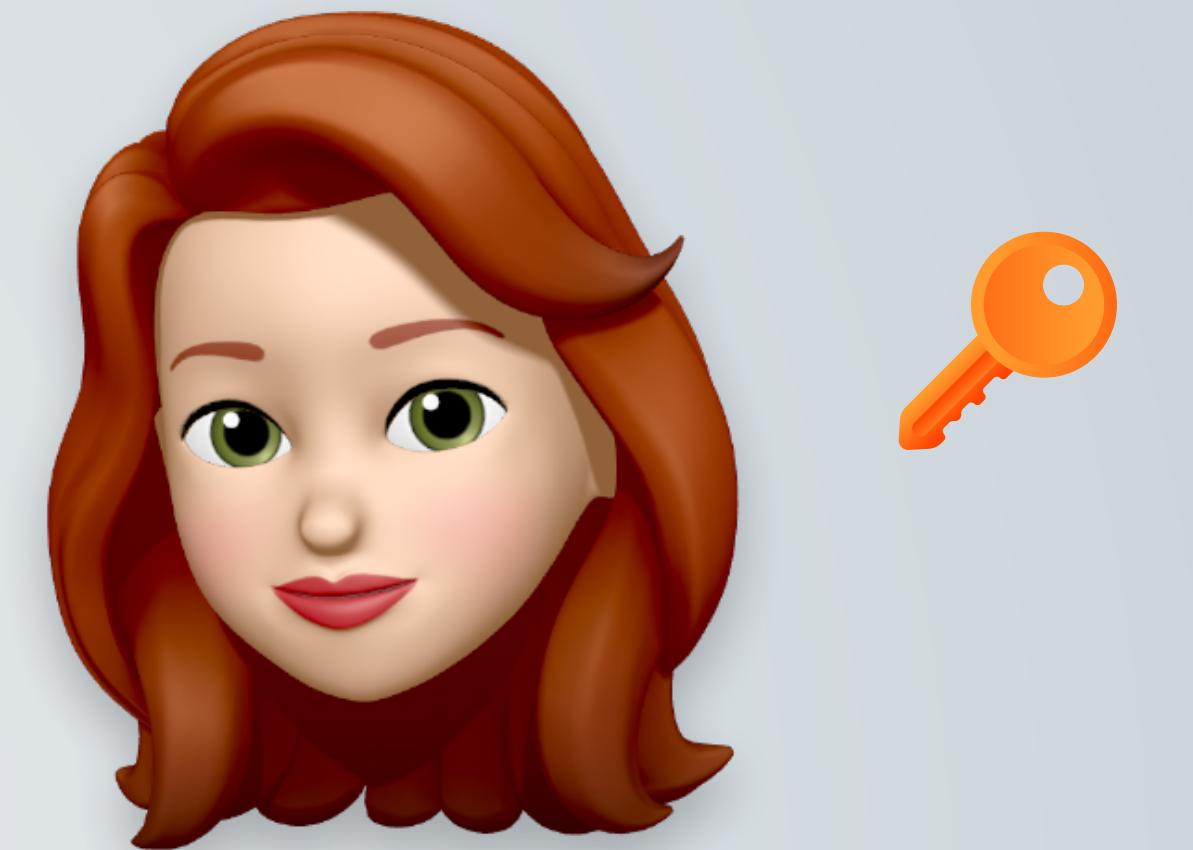
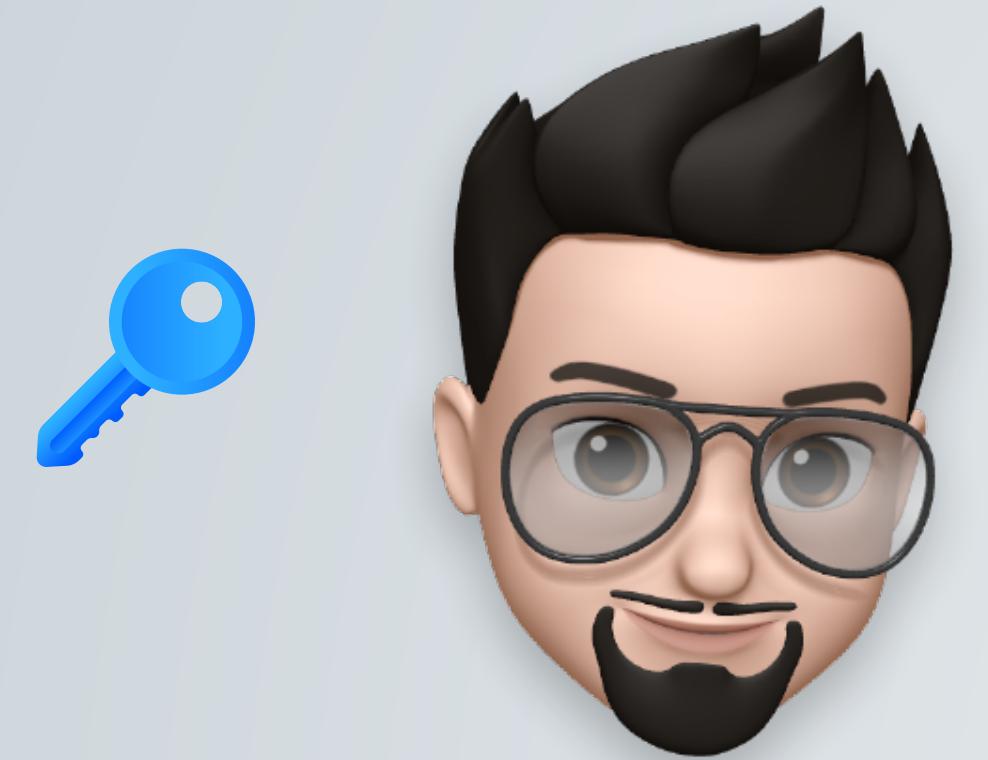
Il metodo dei lucchetti



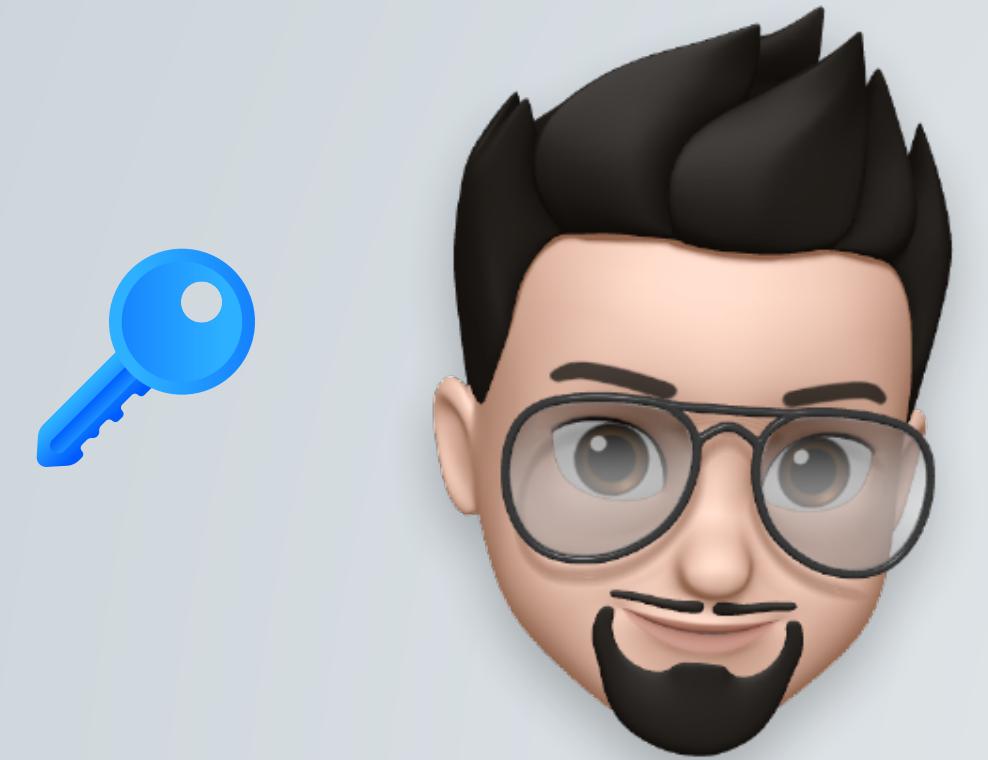
Il metodo dei lucchetti



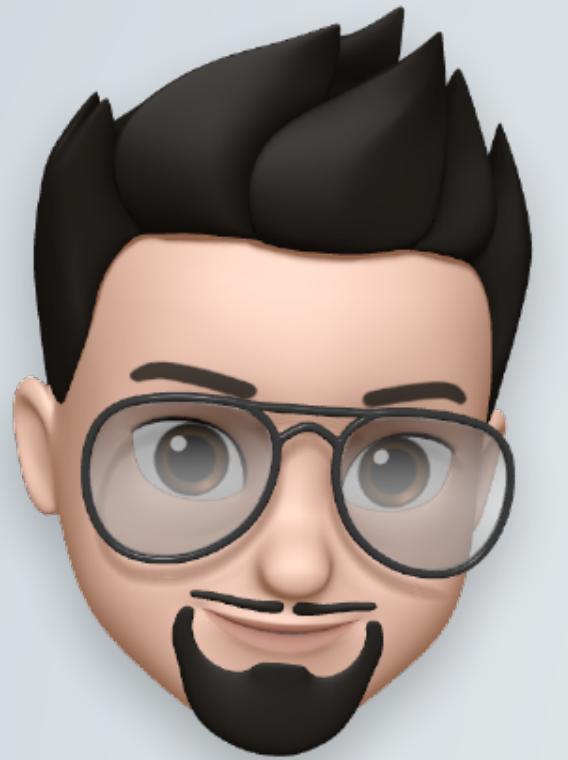
Il metodo dei lucchetti



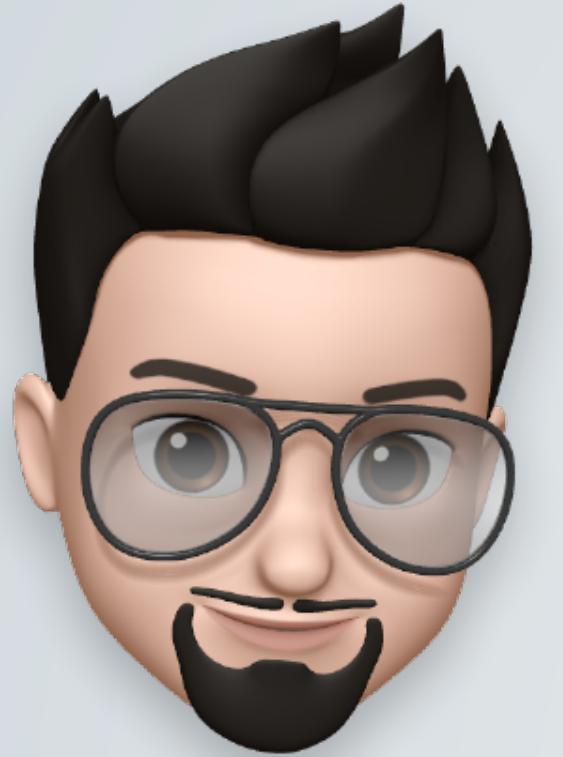
Il metodo dei lucchetti



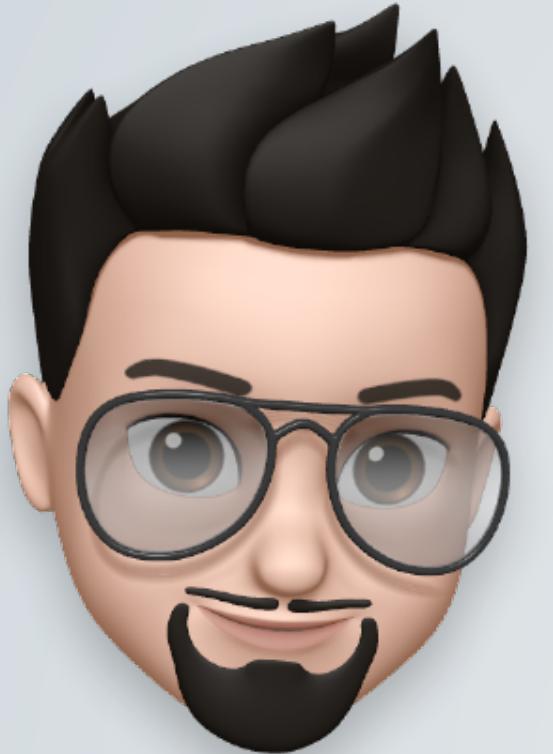
Il metodo dei lucchetti



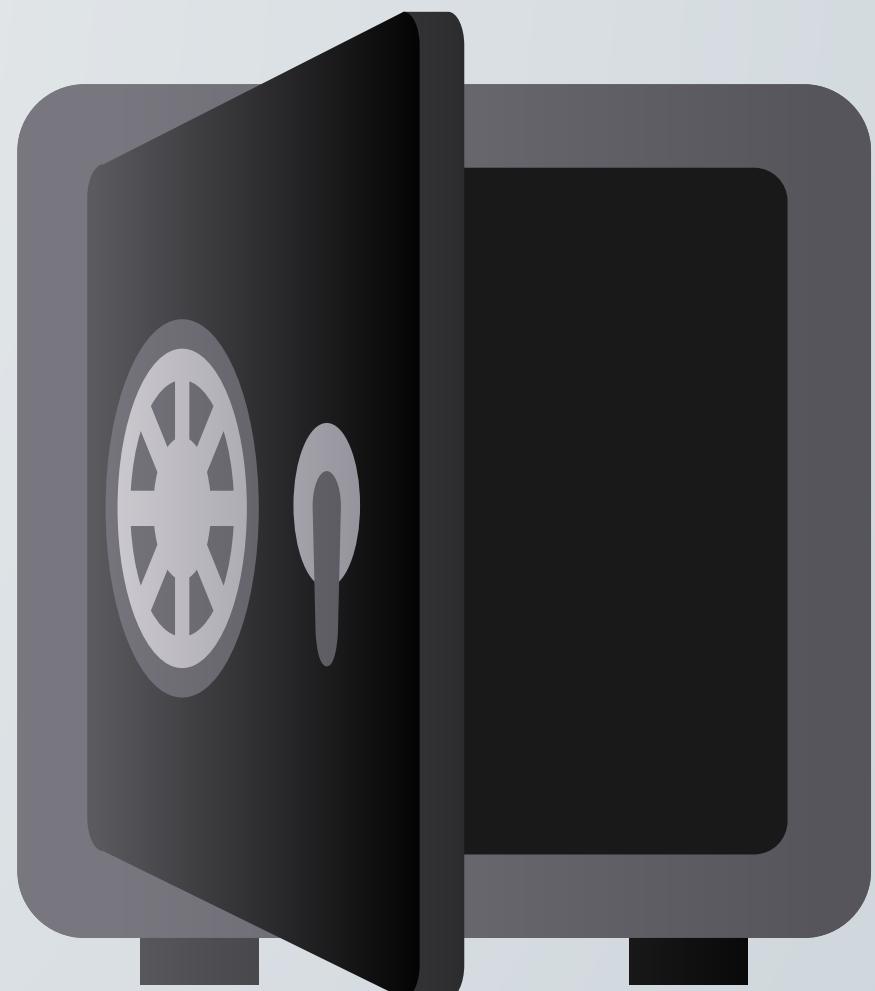
Il metodo dei lucchetti



Il metodo dei lucchetti



Perché questo metodo
non può funzionare?



Composizione di cifrature



Chiave di Bob

abcdefghijklmnopqrstuvwxyz
HFSUGTAKVDEOYJBPNXWCQRIMZL



Chiave di Alice

abcdefghijklmnopqrstuvwxyz
CPMGATNOJEFWIQBURYHXSDZKLV

Messaggio

ci vediamo all una

Cifrato da Bob

SV RGUVHYB HOO QJH

Cifrato da Alice

HD YNSDOLP OBB REO

Decifrato da Bob

AJ MQCJLZP LOO VKL

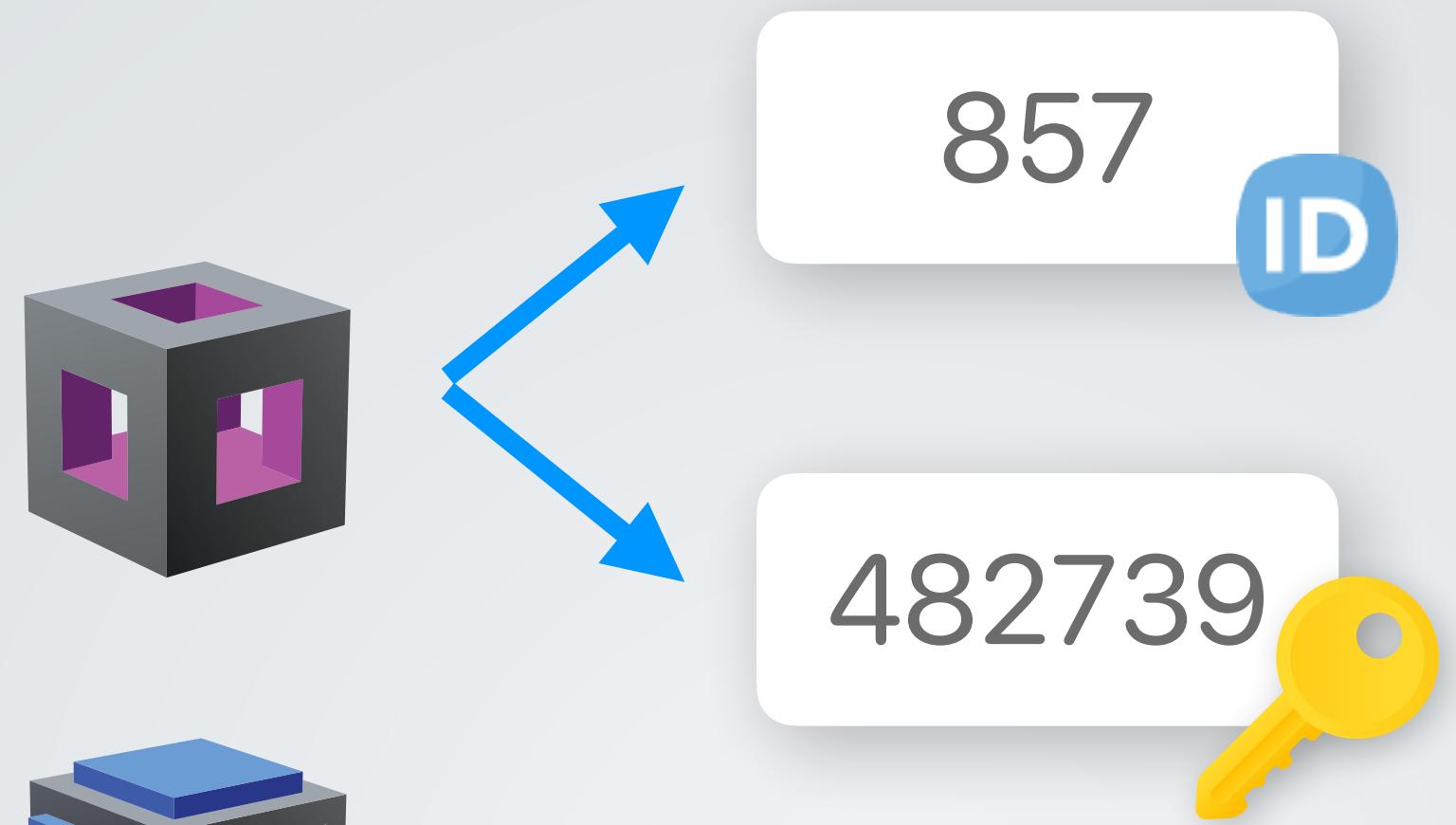
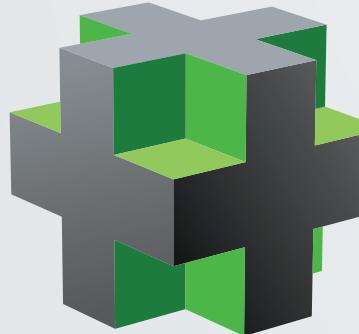
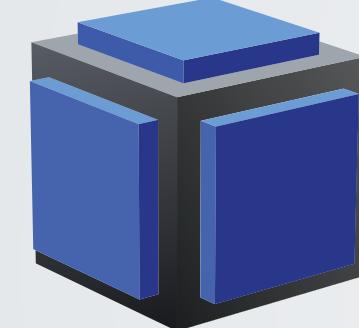
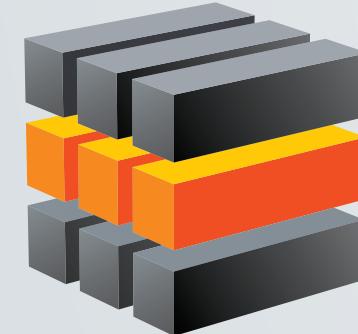
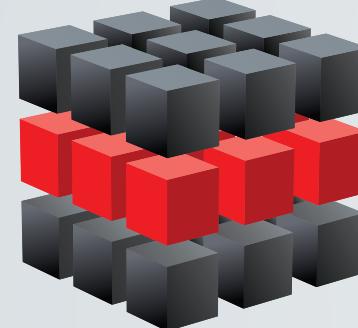
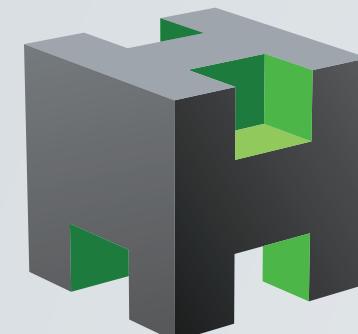
Decifrato da Alice

ei cnaiywbg yhh zxy

I puzzle di Merkle



I puzzle di Merkle

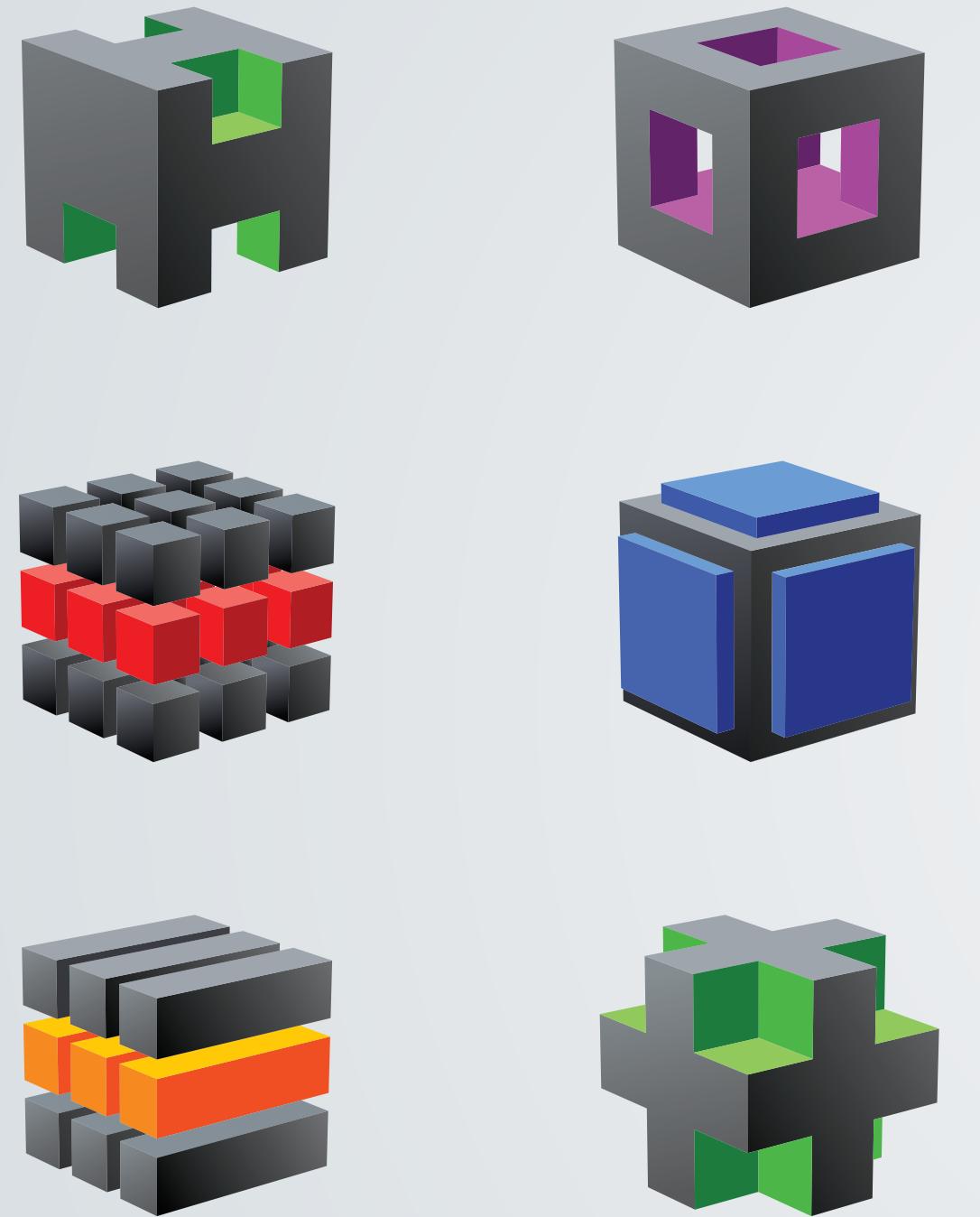


Ogni puzzle, se risolto,
contiene un ID e una
chiave casuale.

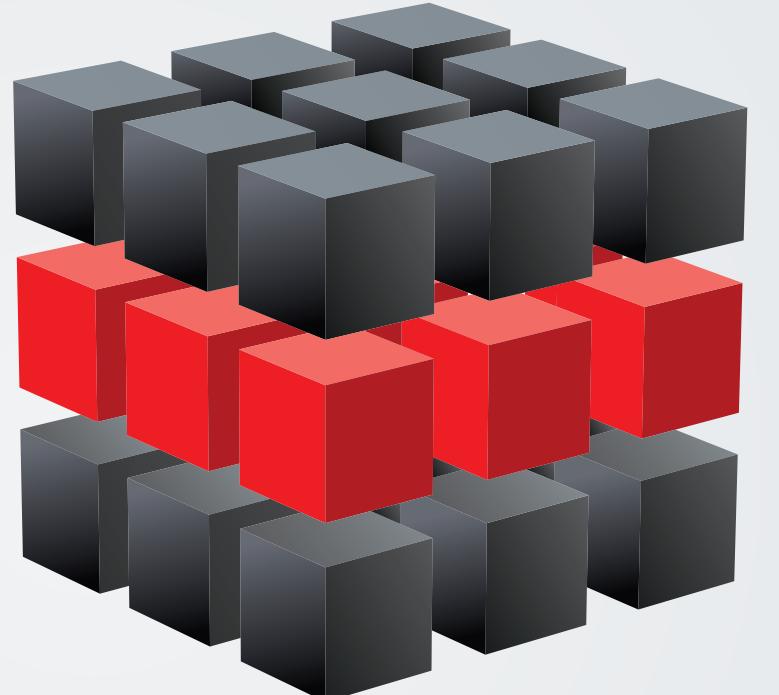


Bob genera 2^n puzzle e
li pubblica.

I puzzle di Merkle



Bob genera 2^n puzzle e li pubblica.

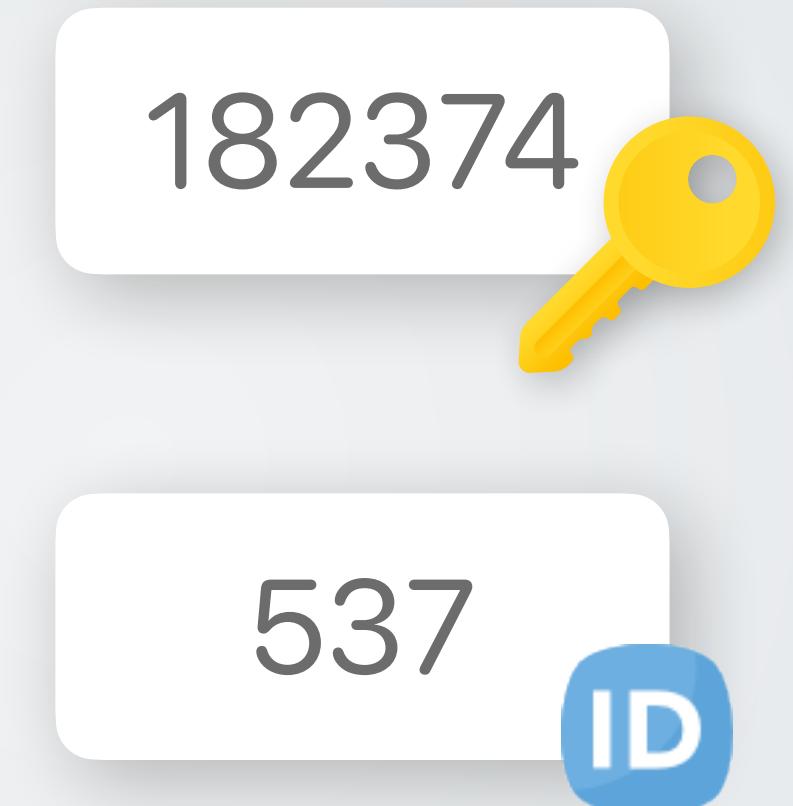
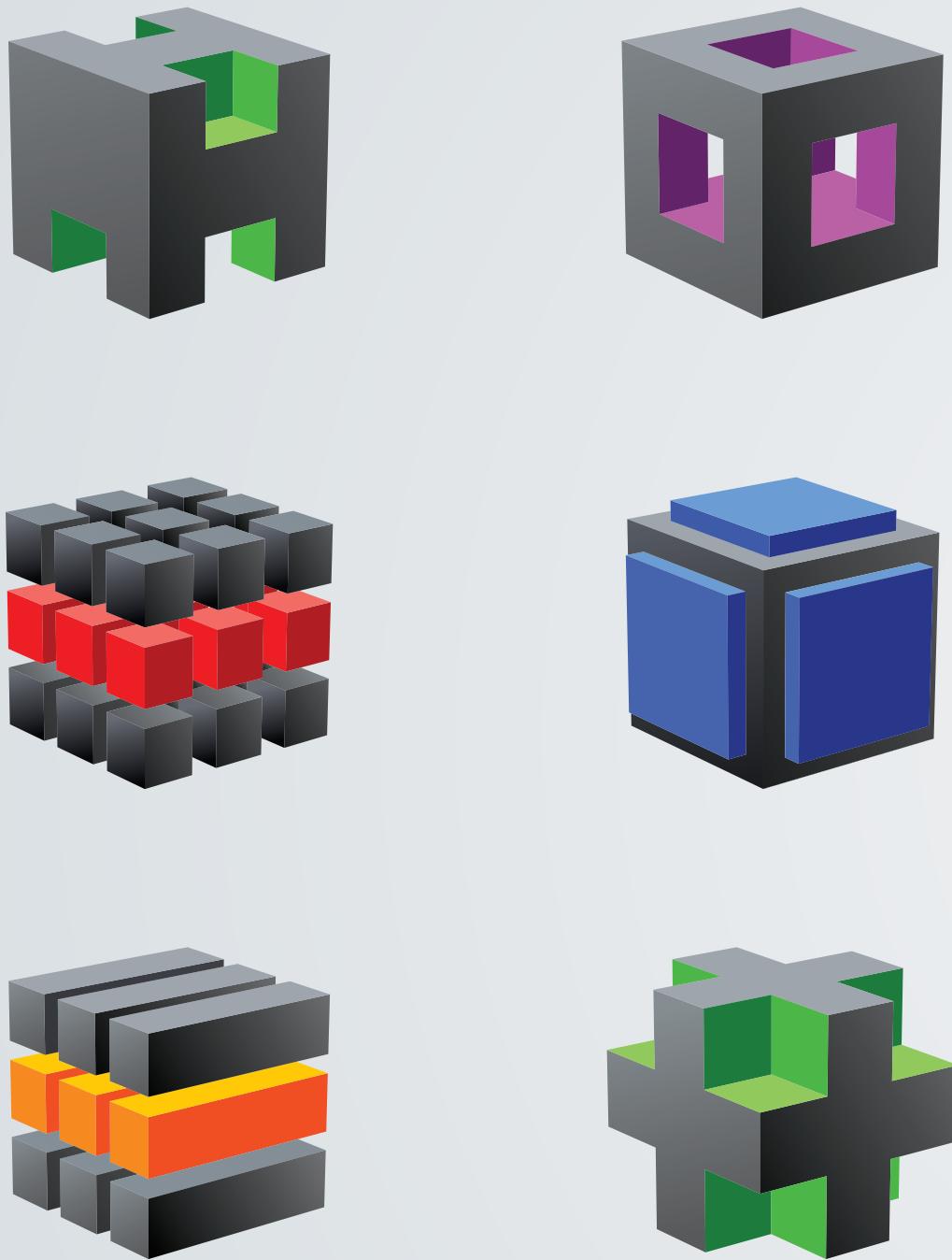


Alice sceglie casualmente un puzzle

I puzzle di Merkle



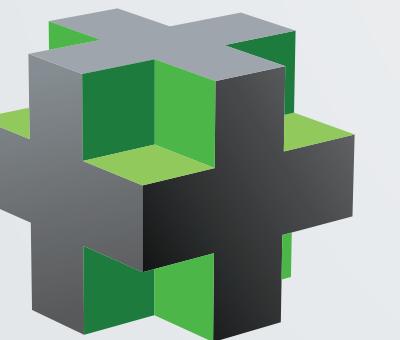
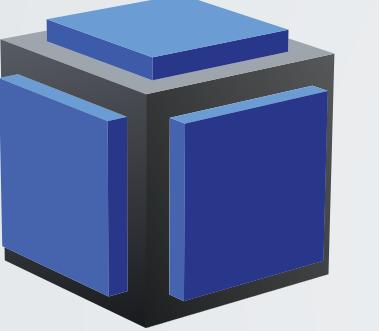
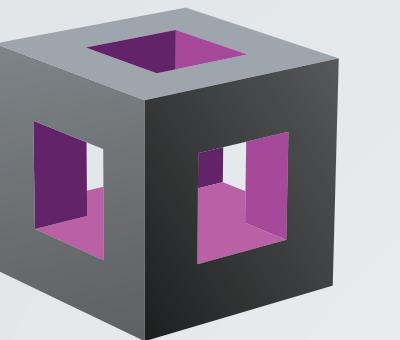
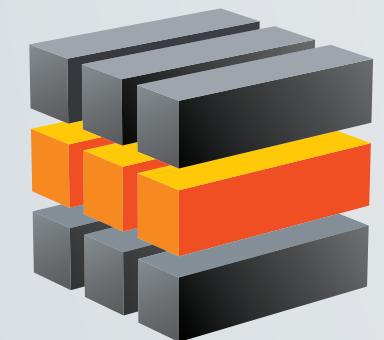
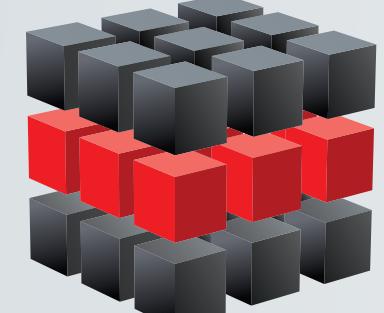
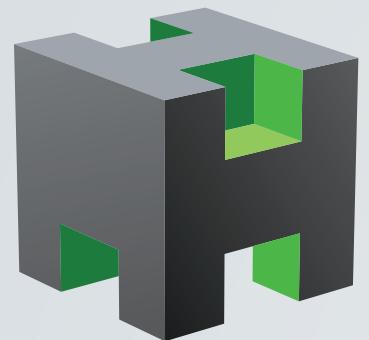
Bob genera 2^n puzzle e li pubblica.



Alice sceglie casualmente un puzzle ...e lo risolve.

I puzzle di Merkle

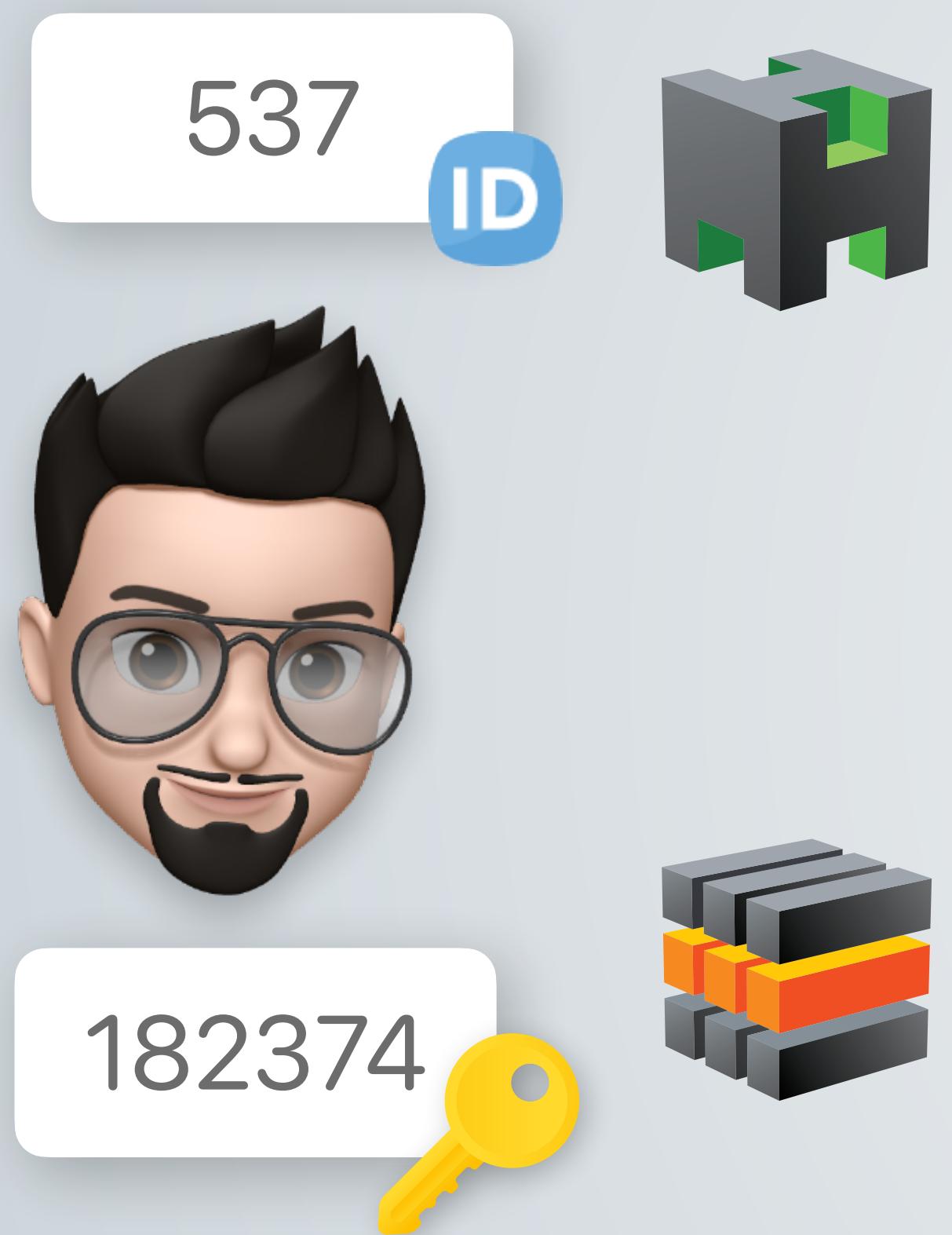
537
ID



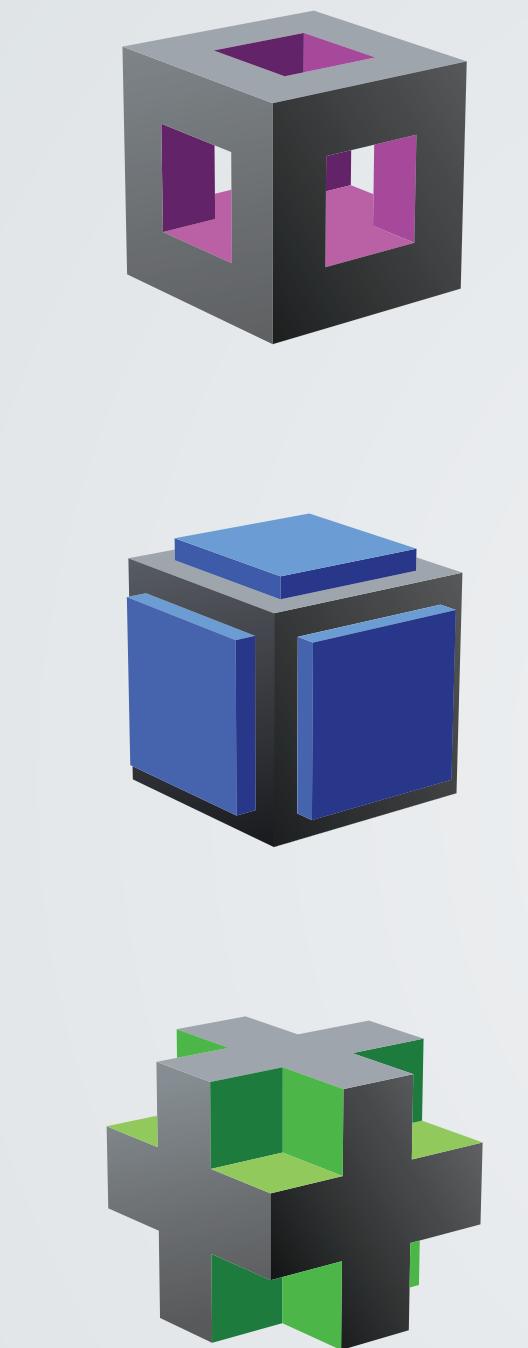
182374
key

Alice invia l'ID a Bob e
tiene copia della chiave

I puzzle di Merkle

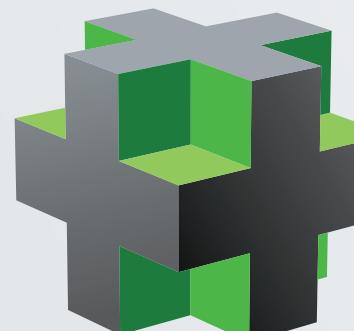
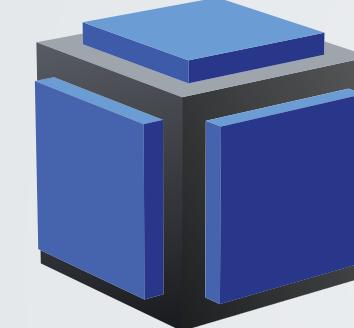
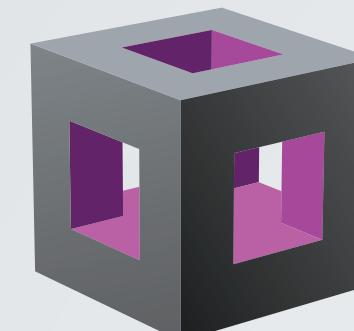
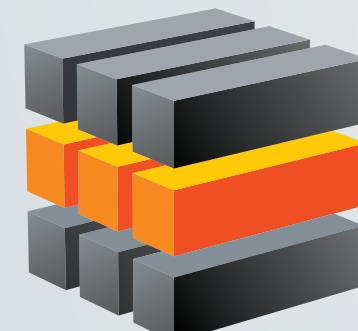
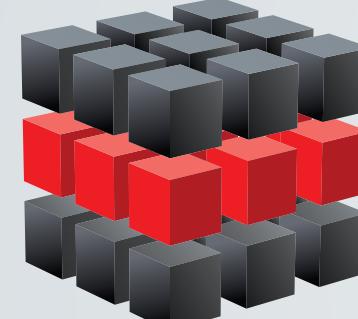
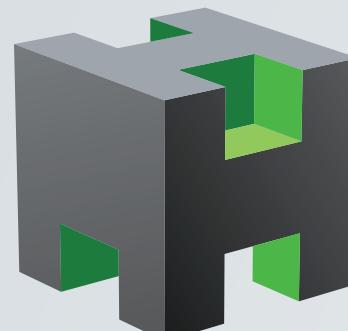


Bob sa quale puzzle risolvere
per ottenere la chiave



Alice invia l'ID a Bob e
tiene copia della chiave

I puzzle di Merkle



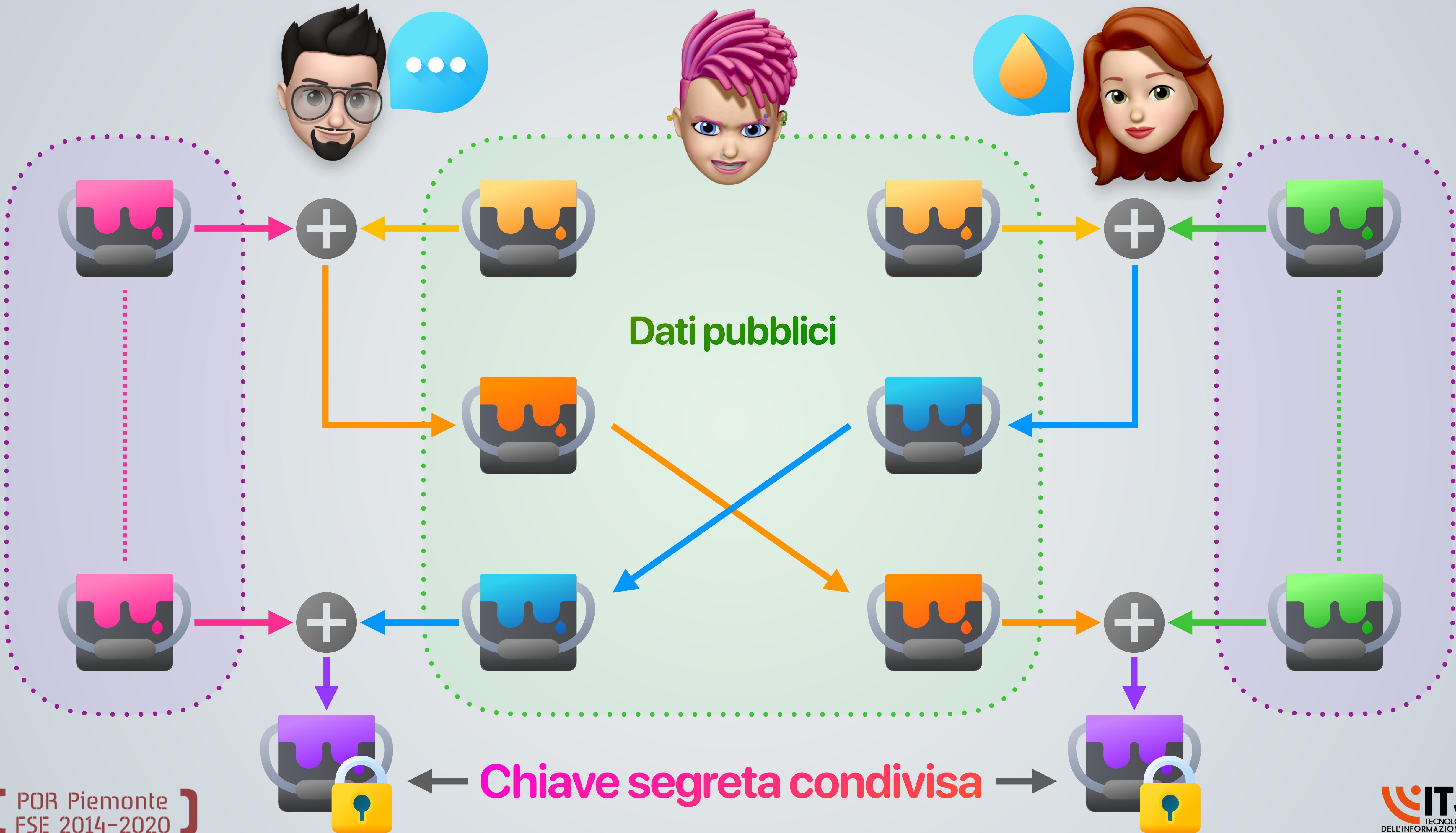
537
ID



L'attaccante può intercettare l'ID, ma deve risolvere tutti i puzzle per scoprire la chiave condivisa.

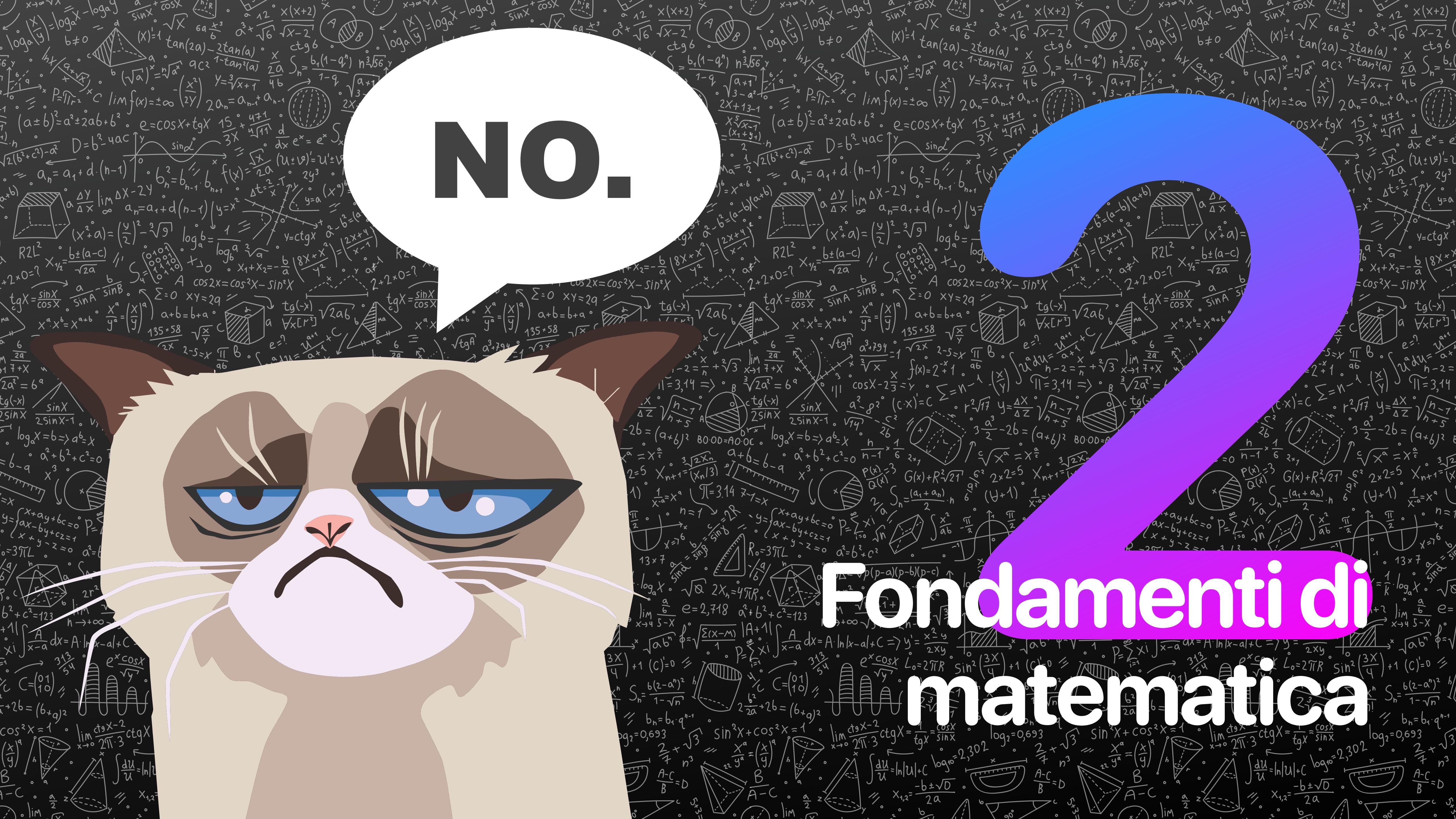


Il metodo dei colori

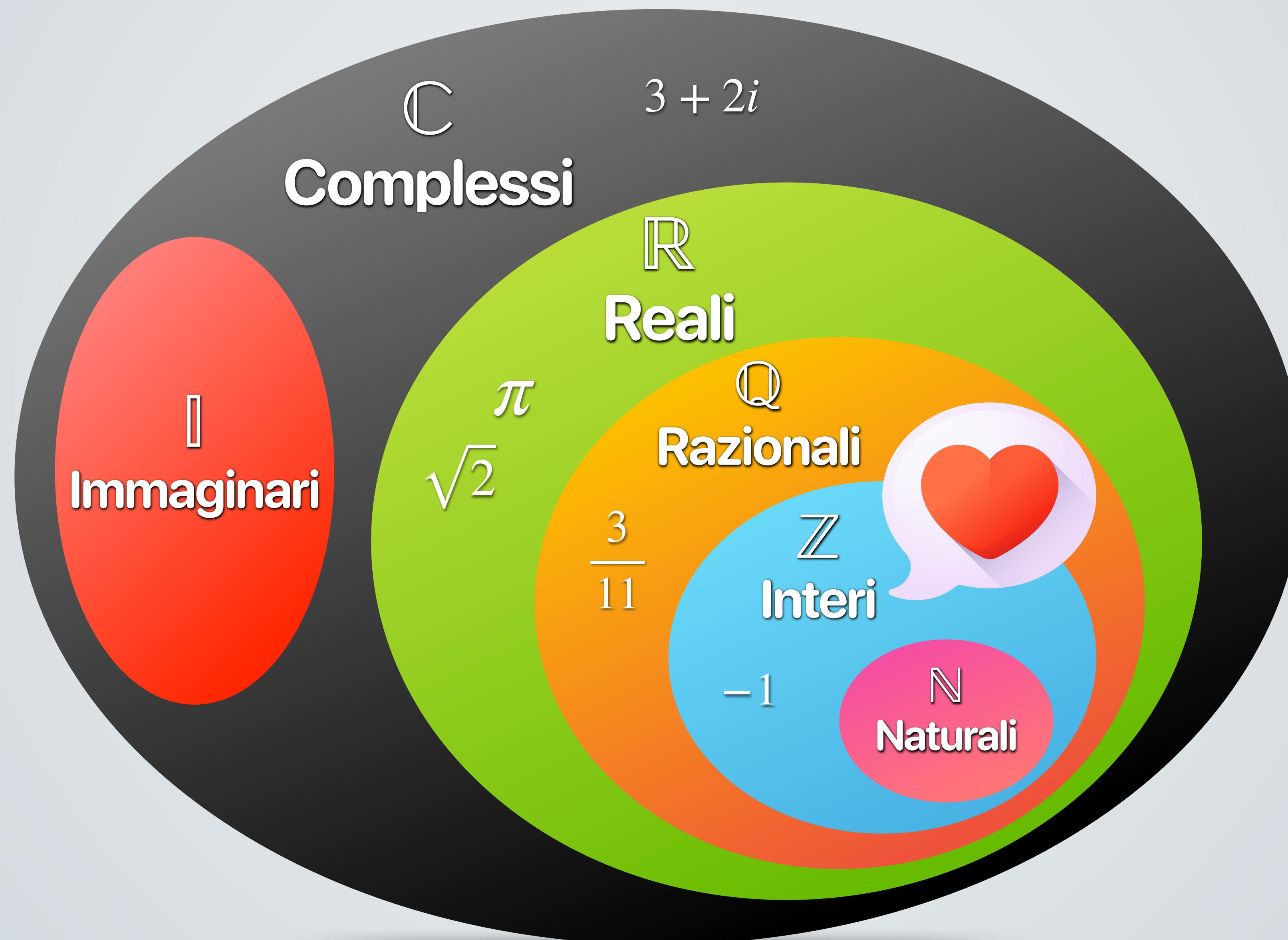


NO.

Fondamenti di matematica



Insiemi numerici



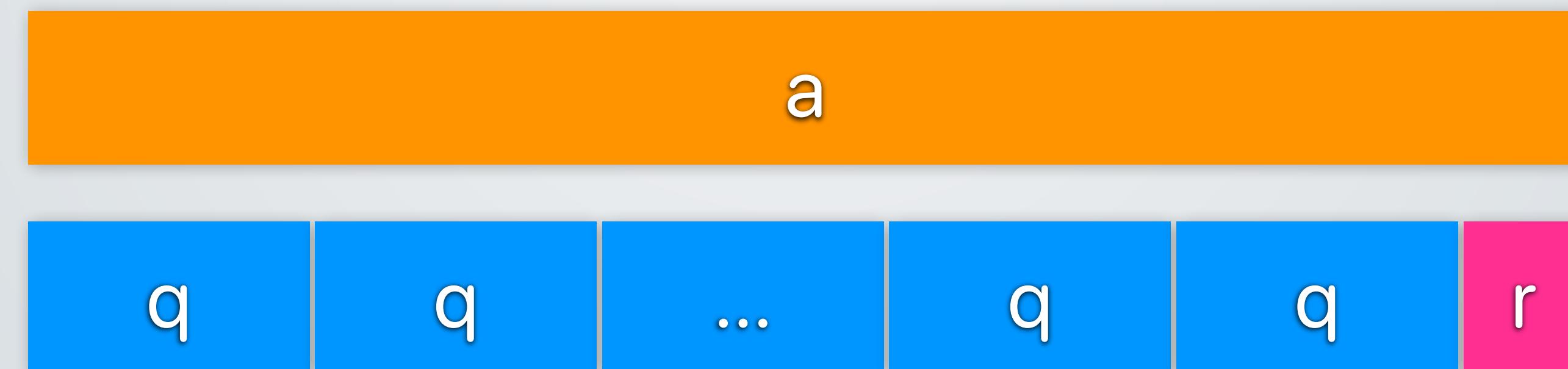


Teorema della divisione

Se $a \geq 0$ e $b > 0$ sono interi, esistono e sono univocamente determinati gli interi $q \geq 0$ ed r tali che

$$a = bq + r \quad \text{e} \quad 0 \leq r < |b|$$

q ed r sono detti rispettivamente il **quoziente** e il **resto** della divisione.



b blocchi grandi q più un certo resto r .



I numeri primi

Un numero intero p si dice primo se:

- $p \neq \{-1, 1, 0\}$;
- per ogni $a \in \mathbb{Z}$, se a divide p , allora $a \in \{-1, 1, p, -p\}$.

In altre parole, un intero è un primo se è diverso da $\{-1, 1, 0\}$ e non ha **divisori propri**.



Teorema fondamentale dell'aritmetica

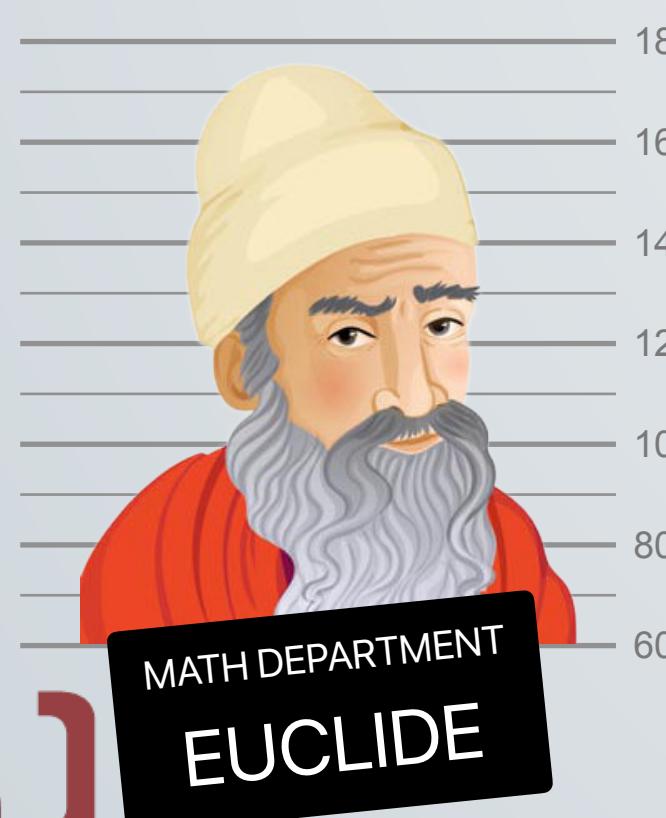


Fattorizzazione

Sia $z \in \mathbb{Z}$ un intero diverso da $\{-1, 0, 1\}$. Allora esistono numeri primi p_1, p_2, \dots, p_n tali che

$$z = p_1 \cdot p_2 \cdot \dots \cdot p_n$$

Inoltre tale **fattorizzazione** è unica, a meno del segno dei numeri primi e del loro ordine nel prodotto.



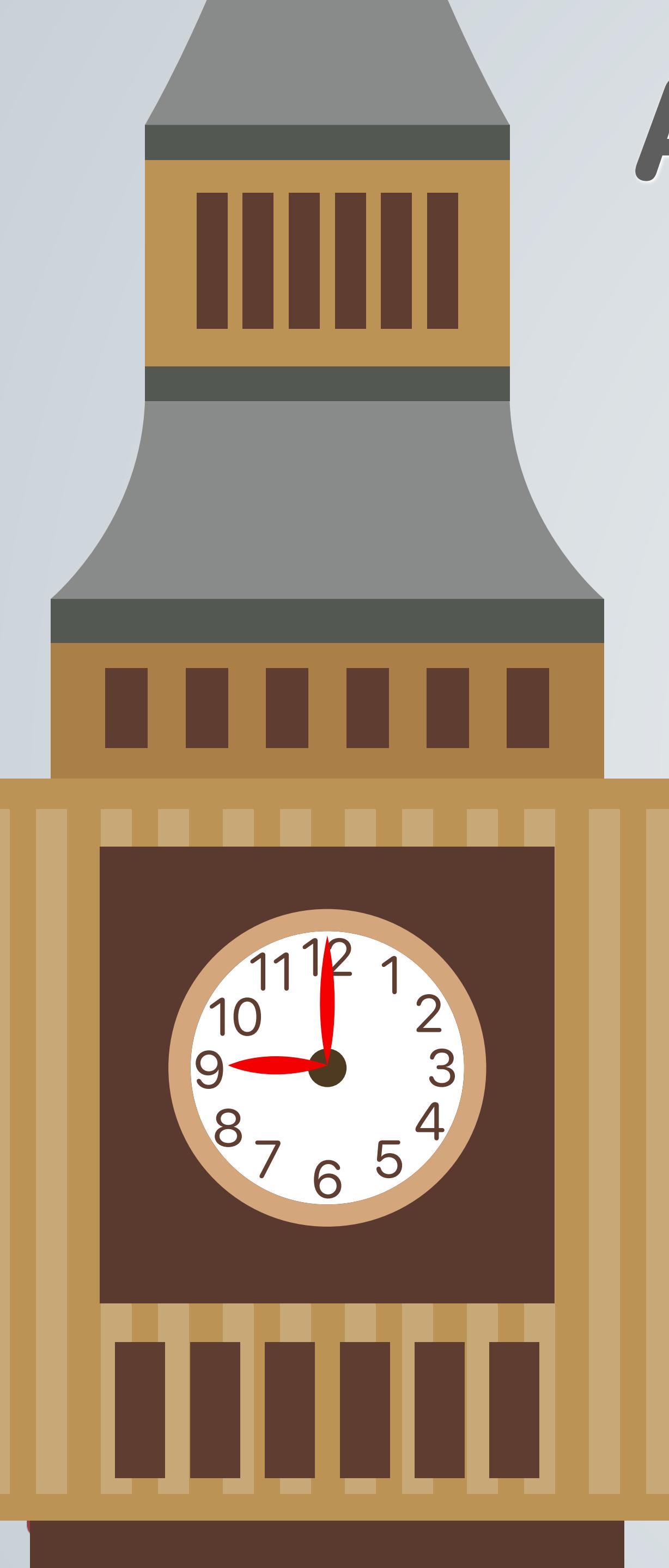
Euclide (Grecia, -III/-V sec.), negli *Elementi*, insieme all'esistenza della fattorizzazione, aveva dimostrato una proposizione, oggi nota come *lemma di Euclide*, dalla quale si ricava la proprietà di fattorizzazione unica.

Il teorema fu poi dimostrato esplicitamente per la prima volta da Gauss nelle *Disquisitiones Arithmeticae*.

Aritmetica dell'orologio

Siamo a Londra e sono le 9 del mattino. Abbiamo un appuntamento tra 8 ore. A che ora abbiamo l'appuntamento?





Aritmetica dell'orologio

Siamo a Londra e sono le 9 del mattino. Abbiamo un appuntamento tra 8 ore. A che ora abbiamo l'appuntamento?

Qual è il rapporto tra il 5 e il 17?

5 è il resto della divisione intera tra 17 e 12!

- Possiamo definire tutte le operazioni aritmetiche nel “mondo dell’orologio”.
- Possiamo astrarre l’idea di orologio e immaginarlo con n ore sul quadrante.



Relazioni di congruenza

Fissiamo un intero n , con $n \geq 2$. I due numeri $a, b \in \mathbb{Z}$ sono detti congruenti modulo n se $n | (b - a)$. In questo caso si scrive

$$a \equiv b \pmod{n}$$

o, equivalentemente, $a \pmod{n} = b$.

Esempio (orologio).

Fissiamo $n = 12$ e scegliamo $a = 3$ e $b = 15$.

Questi numeri sono congruenti in modulo 12 se $12 | (15 - 3)$, che è vero. Dunque:

$$3 \equiv 15 \pmod{12}$$



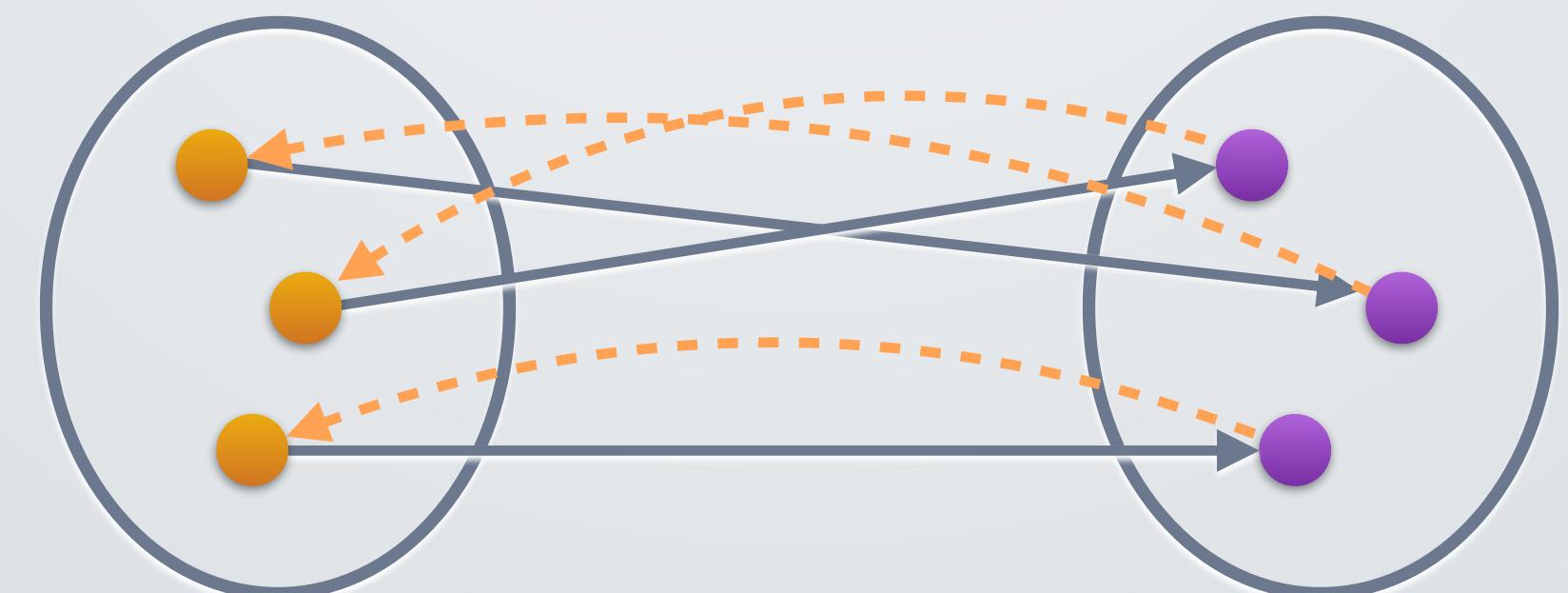
Invertibilità di una funzione

Se una funzione $f: X \rightarrow Y$ è sia iniettiva che suriettiva, allora esiste una corrispondenza biunivoca tra i due insiemi X e Y .

Si può in questo caso definire la funzione inversa

$$f^{-1}(y) \iff f(x) = y$$

Una funzione viene detta **unidirezionale** (*one-way function*) se è computazionalmente difficile da invertire.





Diffie-Hellman-Merkle Key Exchange

Diffie, Hellman e Merkle



Ralph Merkle

Martin Hellman

Whitfield Diffie

Dopo due millenni di buio il problema dello scambio delle chiavi viene risolto nel 1976.

È il primo metodo pratico per scambiare chiavi crittografiche in un canale insicuro ed è tutt'oggi comunemente usato.

A caccia di funzioni unidirezionali

$$a^n = b$$

$$b = \overbrace{a \cdot a \cdot \dots \cdot a}^{n \text{ volte}}$$

$$a^n \equiv b \pmod{c}$$

$$b = \overbrace{a \cdot a \cdot \dots \cdot a}^{\text{Quante volte?}}$$

Non esiste un modo facile per calcolarlo!
Bisogna provare tutti i numeri!

Esempio

Problema: $3^x \bmod 7 = 1$

Soluzione: $x = 6n, n \in \mathbb{Z}, n \geq 0$

$$3^1 \bmod 7 = 1$$

$$3 = 7 \cdot 0 + 3$$

Nope.

$$3^2 \bmod 7 = 1$$

$$9 = 7 \cdot 1 + 2$$

Nope.

$$3^3 \bmod 7 = 1$$

$$27 = 7 \cdot 3 + 6$$

Nope.

$$3^4 \bmod 7 = 1$$

$$81 = 7 \cdot 11 + 4$$

Nope.

$$3^5 \bmod 7 = 1$$

$$243 = 7 \cdot 34 + 5$$

Nope.

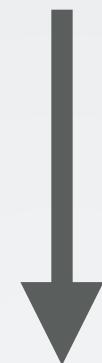
$$3^6 \bmod 7 = 1$$

$$729 = 7 \cdot 104 + 1$$

F**k yeah!

La funzione “logaritmo discreto”

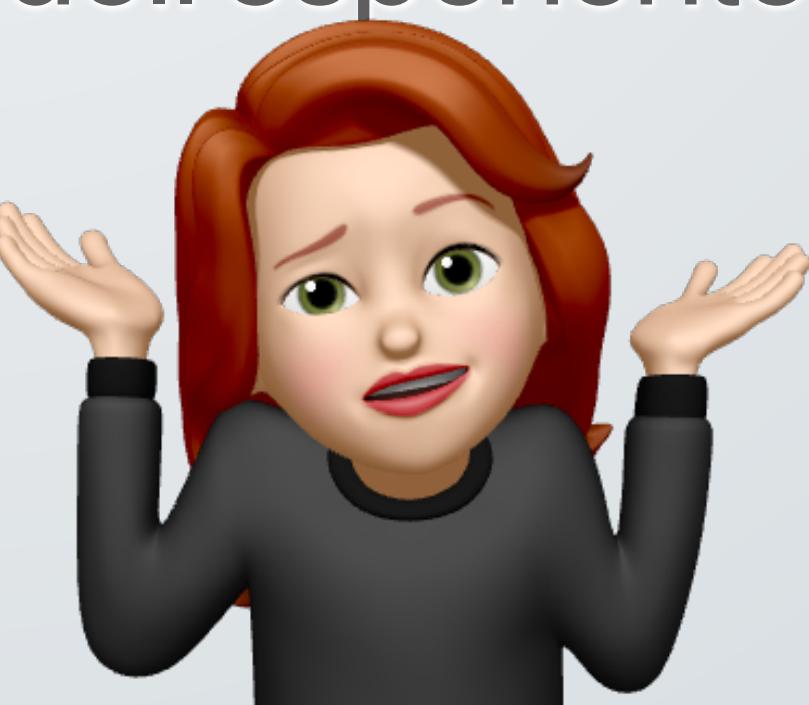
$$a^x = b \pmod{n}$$



$$g^i = b \pmod{p}$$

Il modulo è un **numero primo** p e la base dell'esponente è un **generatore** di p .

Ma... cosa diavolo è un generatore di p ?



Alla ricerca dei generatori perduti

- Scegliere un numero intero g come candidato;
- Calcolare $g^i \pmod{p}$, dove i sono tutti i numeri da 1 a $p - 1$;
- Se i risultati sono una certa permutazione senza ripetizioni dei numeri da 1 a $p - 1$, allora g è un generatore di p .

Esempio: scegliamo $g = 6$ e $p = 17$. Calcoliamo $6^i \pmod{17}$ con $i = [1, p - 1]$

$$i = 1$$

$$6^1 \pmod{17} = 6$$

$$i = 2$$

$$6^2 \pmod{17} = 2$$

$$i = 3$$

$$6^3 \pmod{17} = 12$$

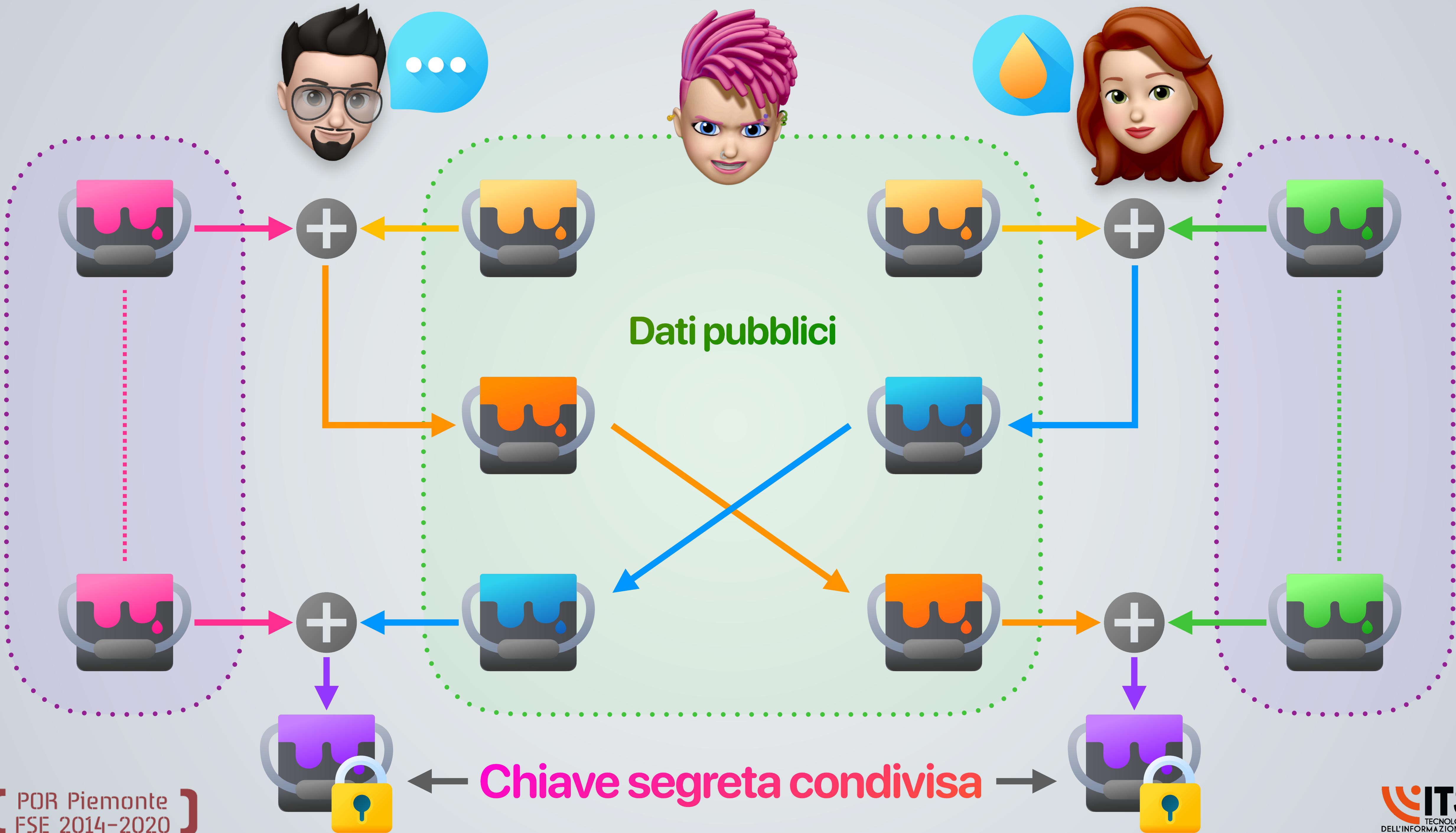
...

$$i = (p - 1)$$

$$6^{16} \pmod{17} = 1$$

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$6^i \pmod{17}$	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

Possiamo quindi verificare che $g = 6$ è un generatore di $p = 17$ poiché è una permutazione senza ripetizioni.



L'algoritmo Diffie-Hellman



Di comune accordo vengono scelti g e p .



$$X_B \in [1, p - 1]$$



$$Y_B = g^{X_B} \pmod{p}$$

$$X_A \in [1, p - 1]$$



$$Y_A = g^{X_A} \pmod{p}$$



$$K = Y_A^{X_B} \pmod{p}$$

$$Y_A$$

**K è la chiave
segreta
condivisa**

$$Y_B$$

$$K = Y_B^{X_A} \pmod{p}$$



L'algoritmo Diffie-Hellman



Di comune accordo vengono scelti $g = 6$ e $p = 17$.



$$X_B = 10 \in [1, 16]$$



$$Y_B = 6^{10} \pmod{17} = 15$$



$$K = 3^{10} \pmod{17} = 8$$

$$X_A = 15 \in [1, 16]$$



$$Y_A = 6^{15} \pmod{17} = 3$$



$$Y_A = 3$$



$$Y_B = 15$$



$$K = 15^{15} \pmod{17} = 8$$



Dimostrazione

Supponiamo per assurdo che $K_A \neq K_B$.

Per definizione sappiamo che $Y_A = g^{X_A} \pmod{p}$ e che $Y_B = g^{X_B} \pmod{p}$.

Sappiamo inoltre che:

$$K_A = Y_B^{X_A} \pmod{p}$$

$$K_B = Y_A^{X_B} \pmod{p}$$

Ora sostituiamo nelle equazioni precedenti le definizioni di Y_A e di Y_B :

$$K_A = (g^{X_B} \pmod{p})^{X_A} \pmod{p}$$

$$K_B = (g^{X_A} \pmod{p})^{X_B} \pmod{p}$$

$$K_A = g^{X_B X_A} \pmod{p}$$

$$K_B = g^{X_A X_B} \pmod{p}$$

Otteniamo che $K_A = K_B$, che contraddice l'ipotesi per assurdo rendendola falsa.

Crittoanalisi

Eve conosce il numero primo $p = 17$, il generatore $g = 6$ e i valori pubblici $Y_A = 3$ e $Y_B = 15$.

A partire da questi dati può calcolare la chiave condivisa K ?



i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$6^i \text{ mod } 17$	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1

Eve deve calcolare tutte le equazioni $g^i \text{ mod } p$ finché non trova Y_A oppure Y_B .

A questo punto il logaritmo discreto è invertito poiché viene individuata la componente segreta X_A oppure X_B .

K può quindi essere facilmente calcolata con la sua equazione.

Perché la procedura è sicura?

Perché nelle implementazioni reali si usano numeri di

300
cifre



Man-in-the-middle
attack

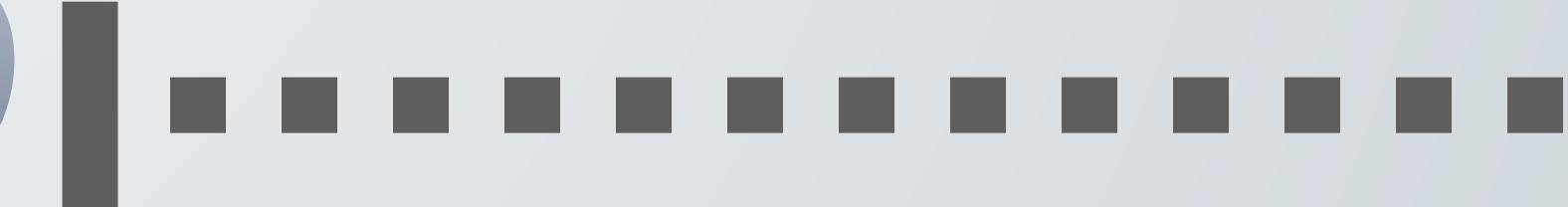
Man-in-the-middle attack



Alice e Bob devono scambiarsi l'informazione pubblica.

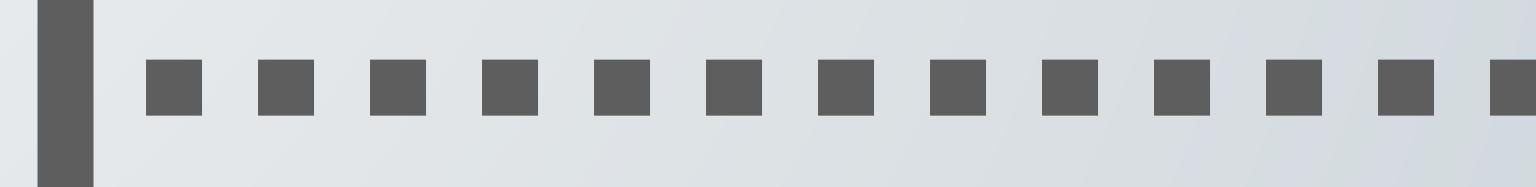
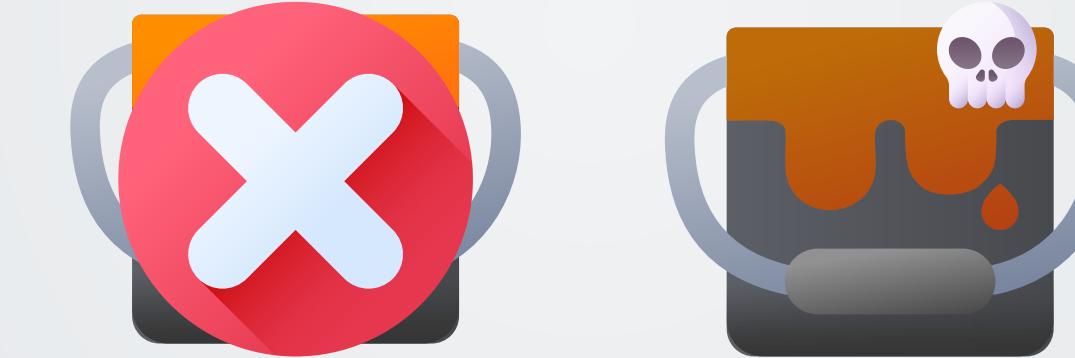
Eve controlla il canale di comunicazione.

Man-in-the-middle attack



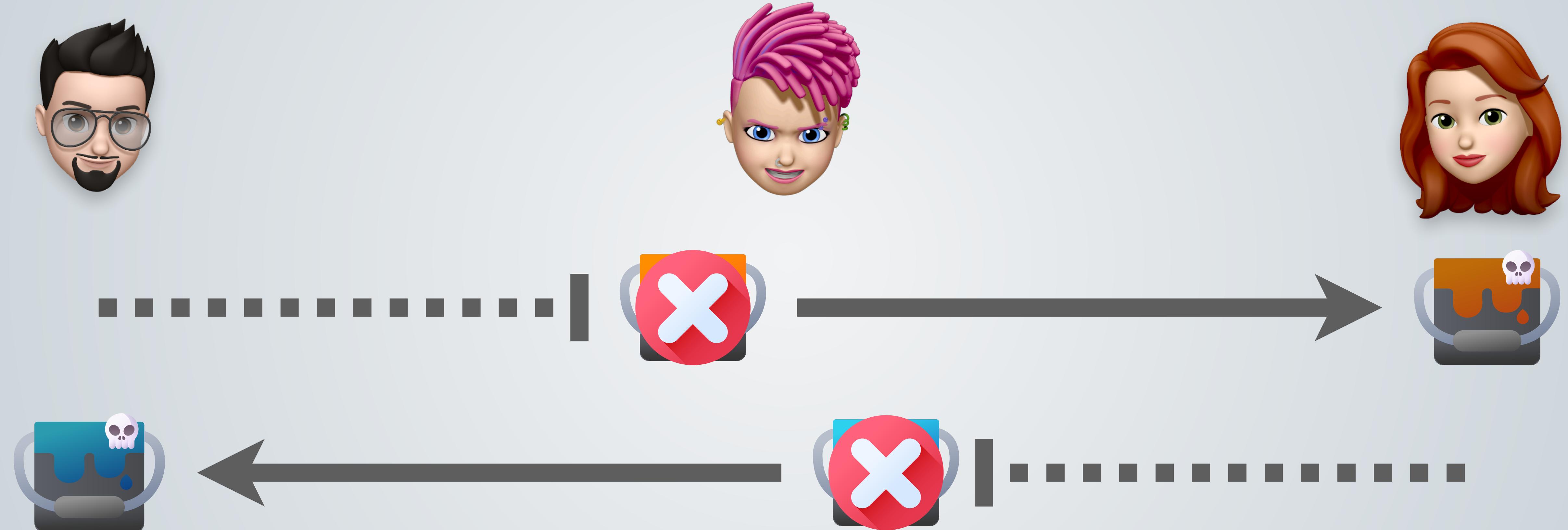
Alice e Bob inviano l'informazione, ma Eve le intercetta.

Man-in-the-middle attack



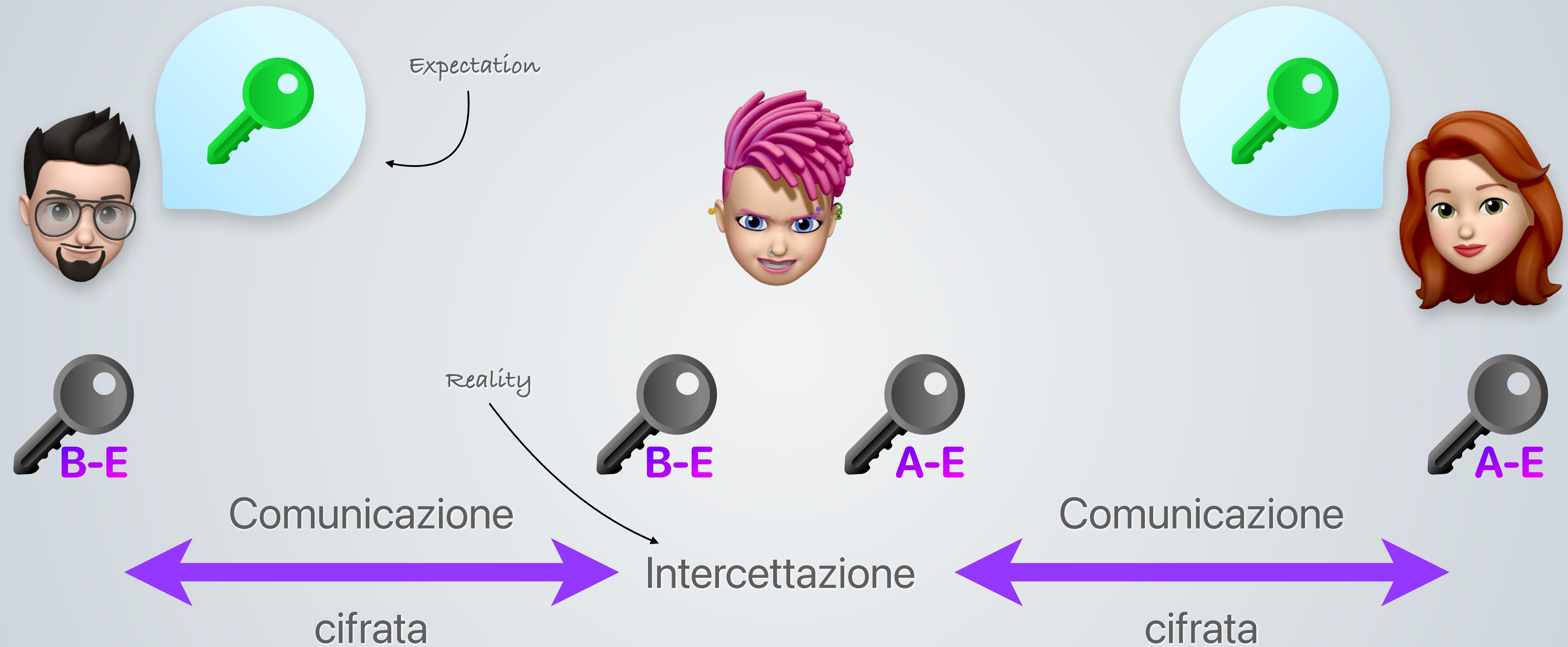
Eve crea delle versioni fraudolente delle informazioni pubbliche di Bob e Alice.

Man-in-the-middle attack



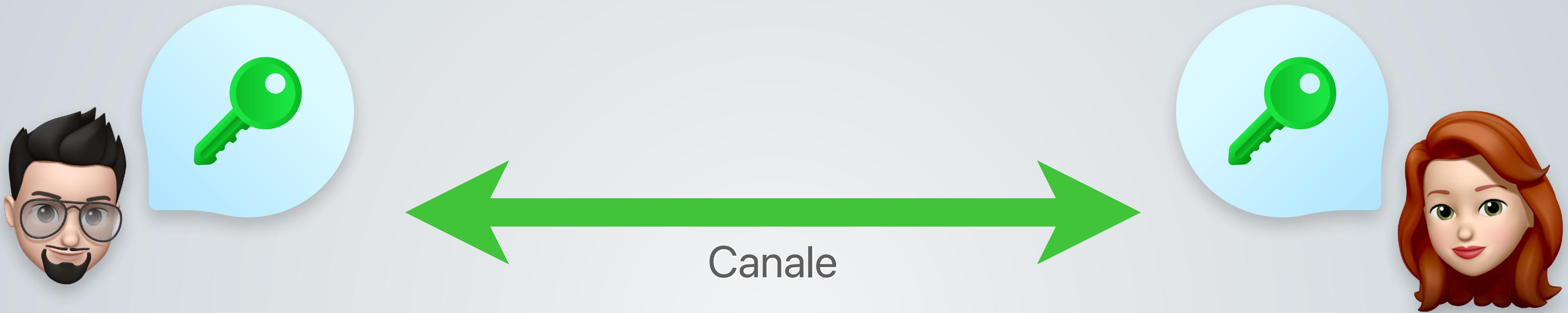
Eve spedisce le versioni fraudolente ingannando entrambi.

Man-in-the-middle attack



Alice e Bob credono di aver condiviso una chiave, ma l'hanno in realtà condivisa con Eve, che ora sta in mezzo alla conversazione e può intercettare tutto.

Risolvere il Man-in-the-middle



Come possiamo verificare che nessuno si sia messo in mezzo alla comunicazione?

Verifica manuale

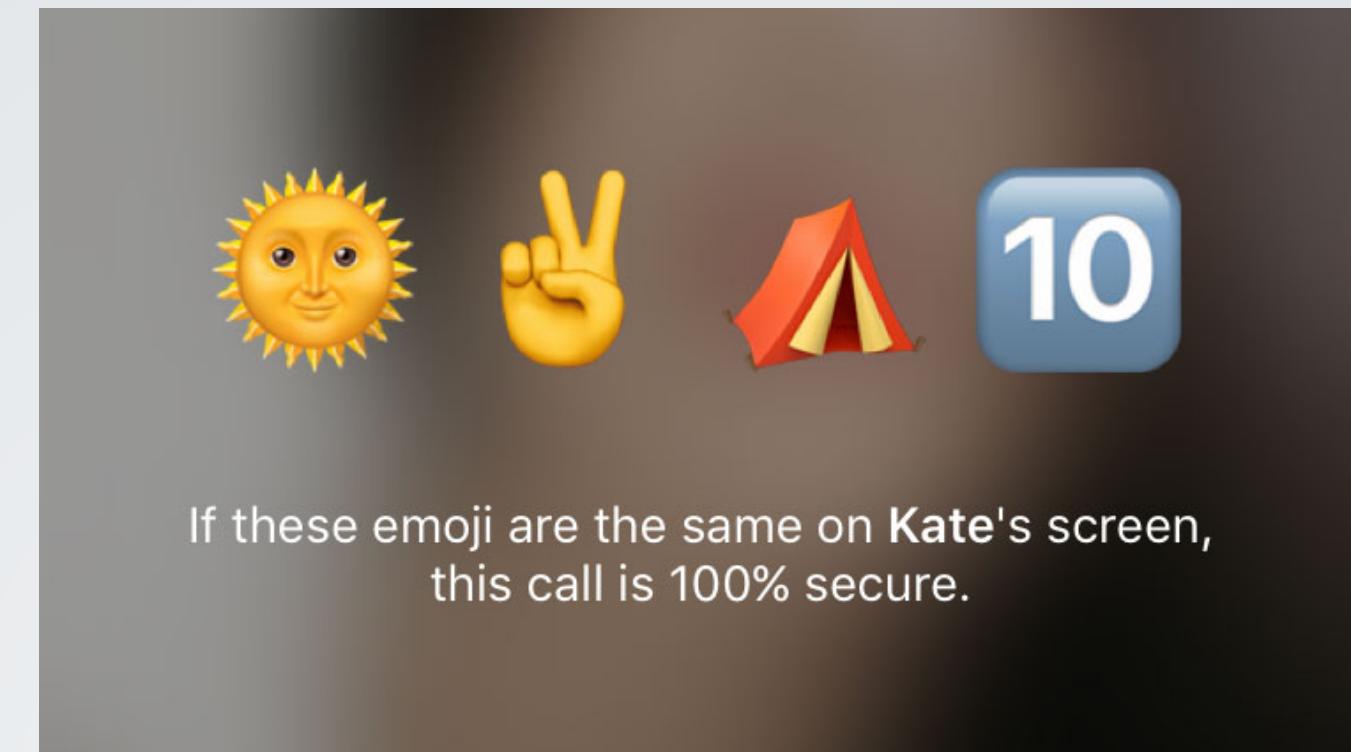
Certificazione

(tra due lezioni...)

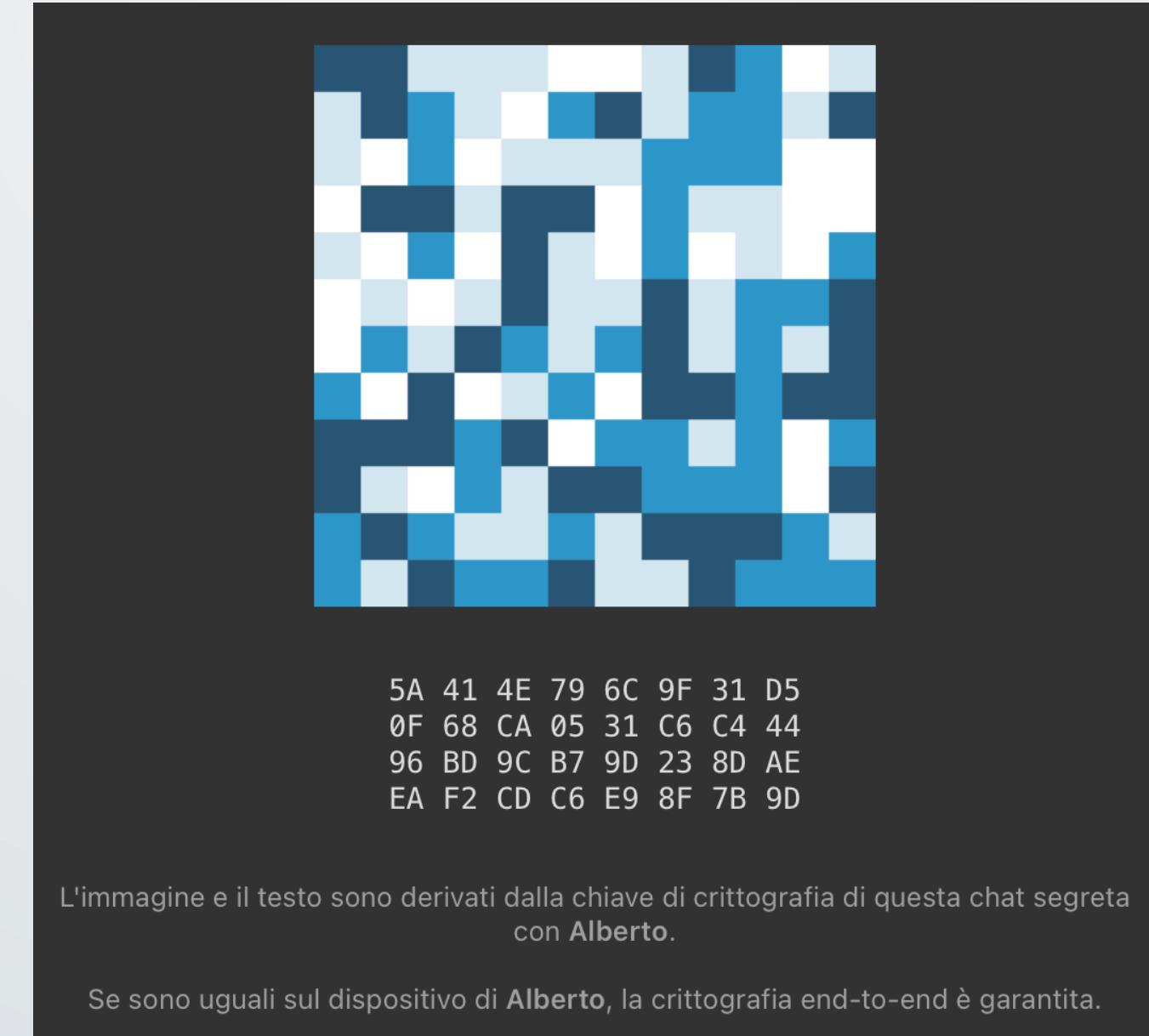
Contromisure: Telegram



@marcofarina

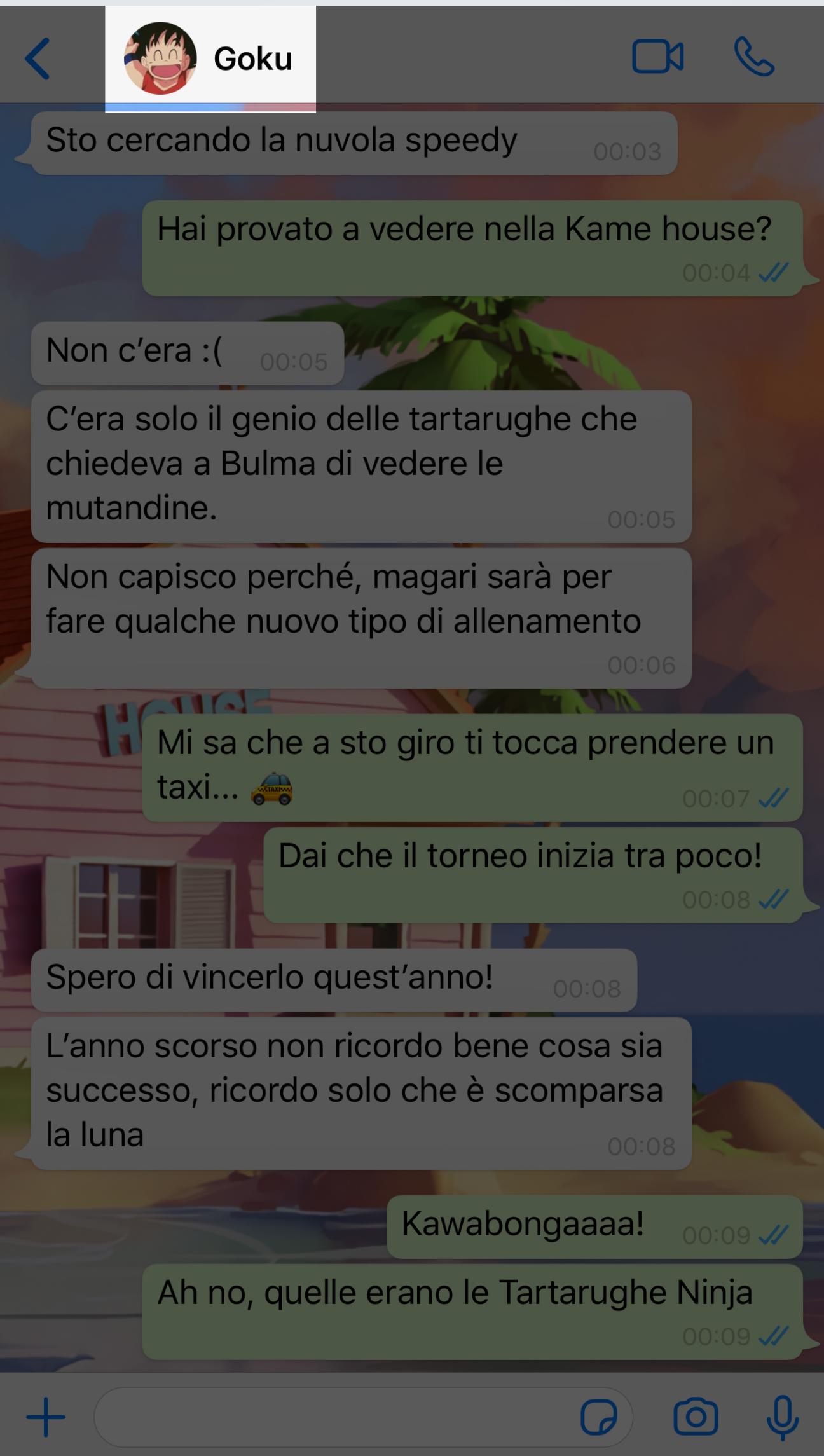


Video call

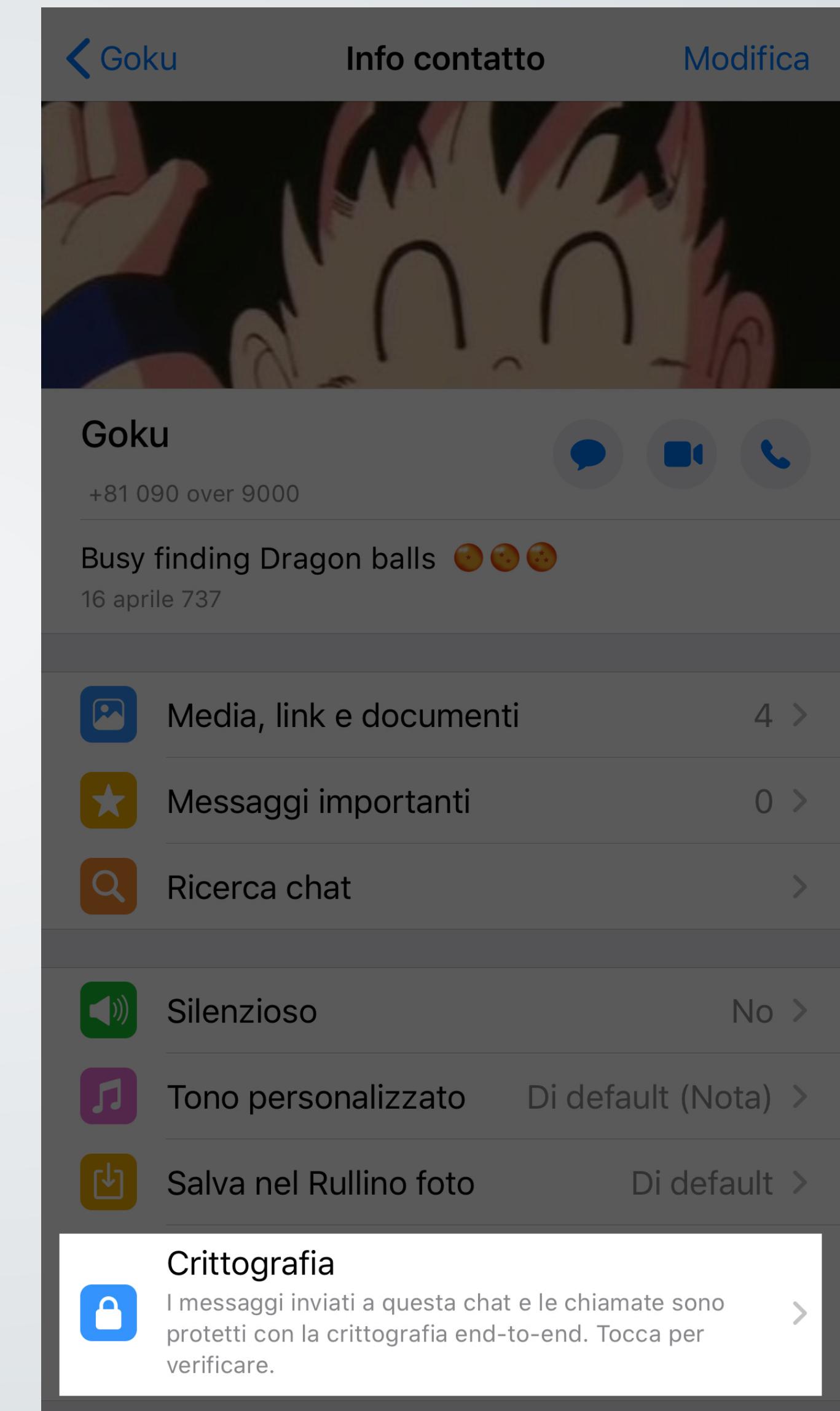
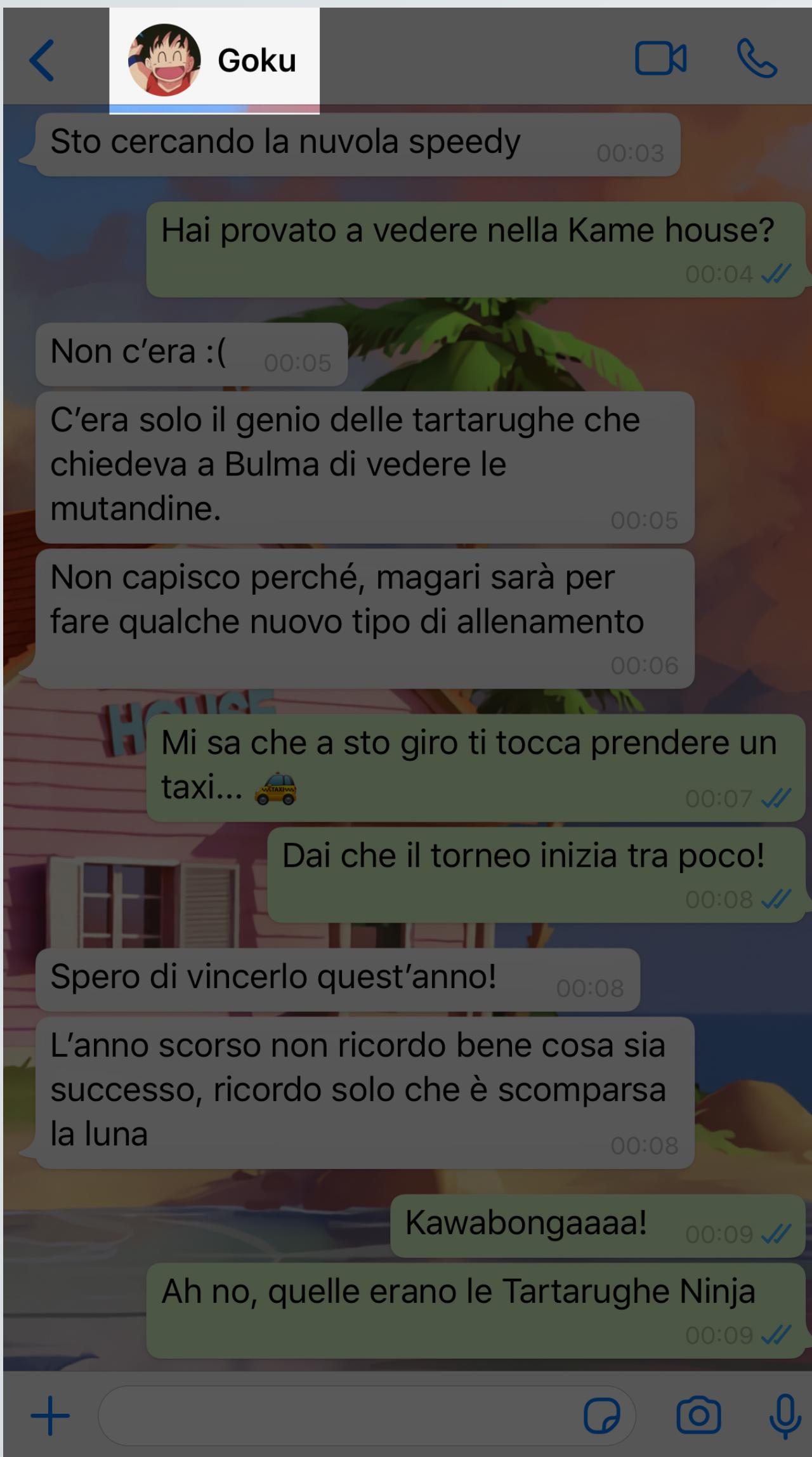


Secret chats

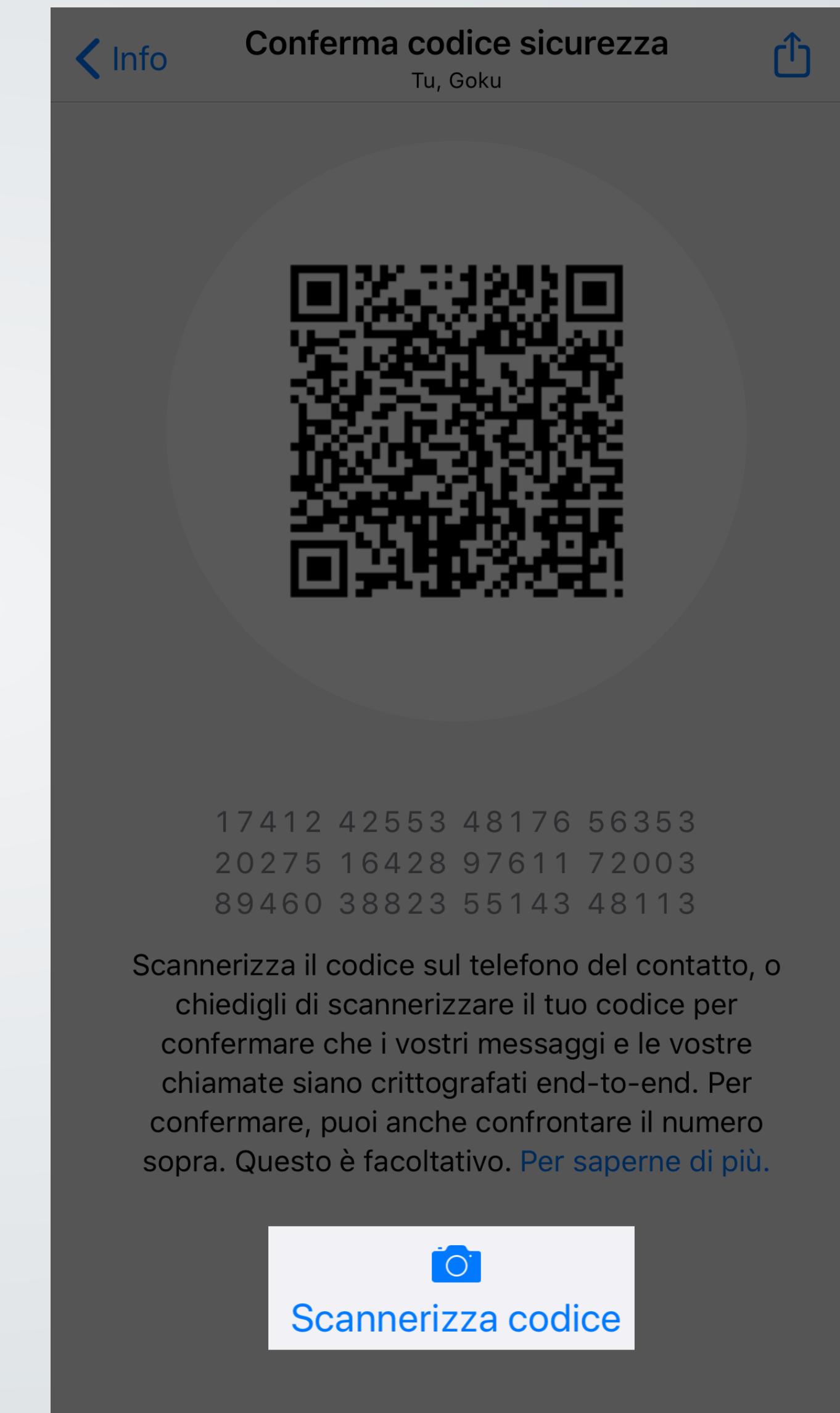
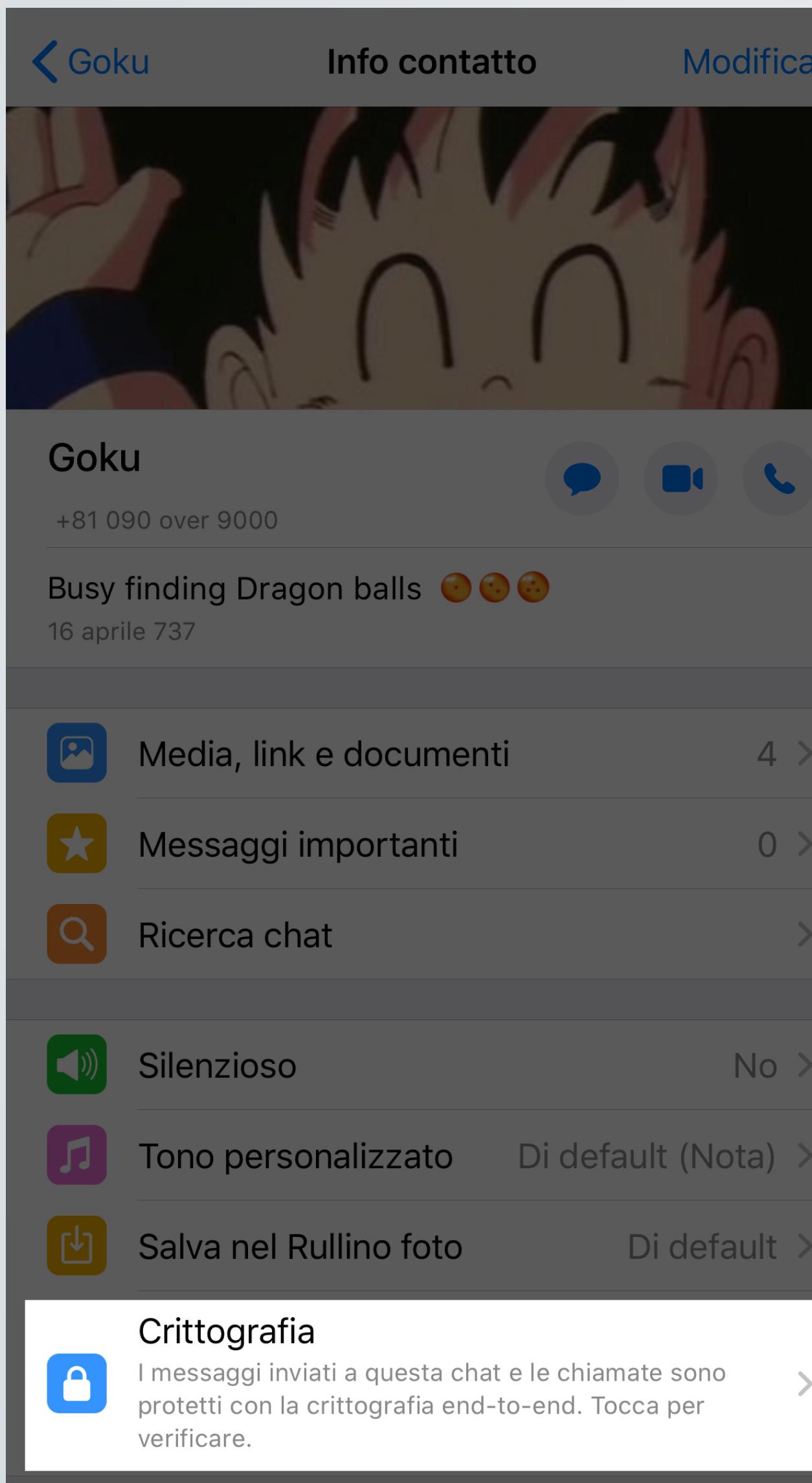
Contromisure: WhatsApp



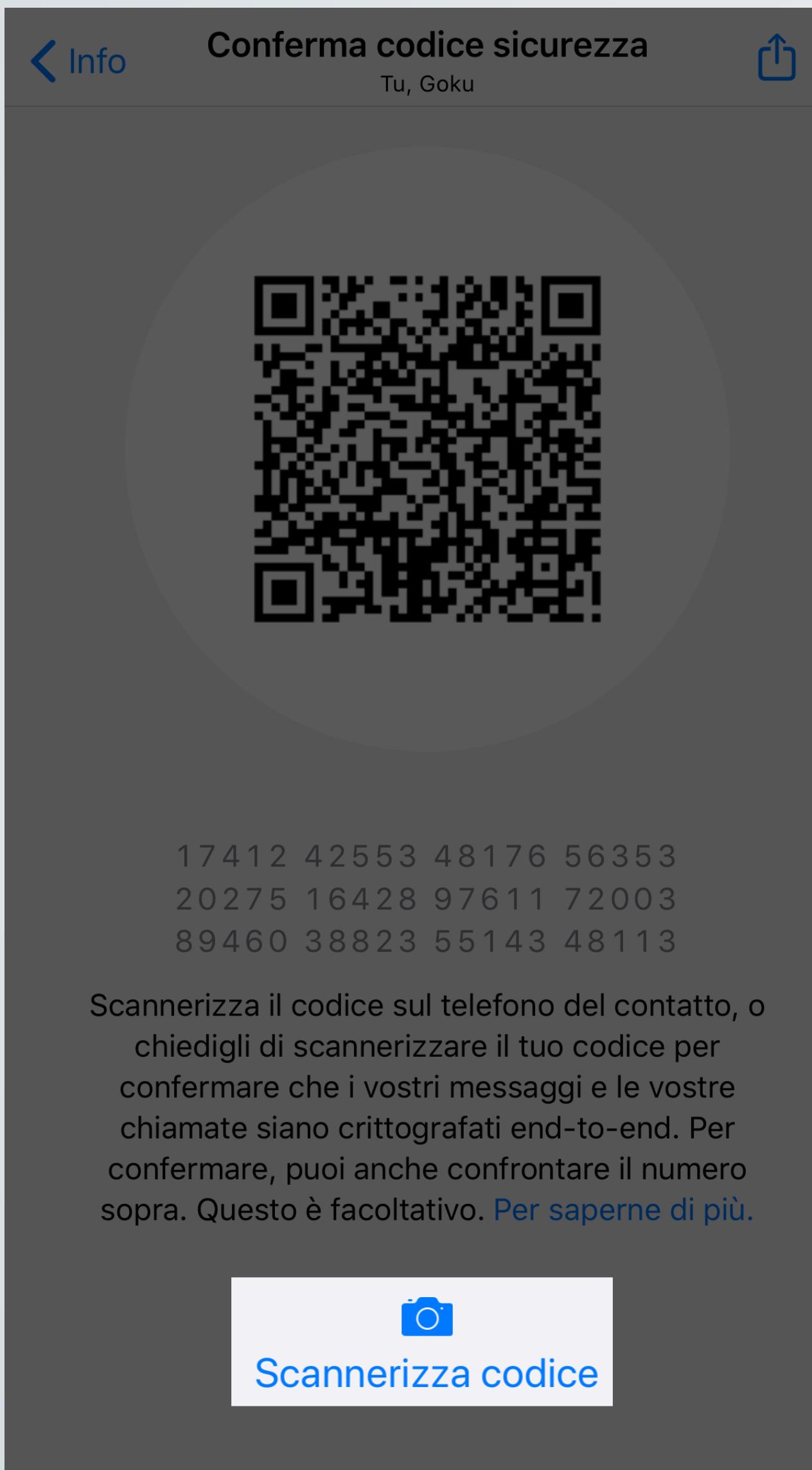
Contromisure: WhatsApp



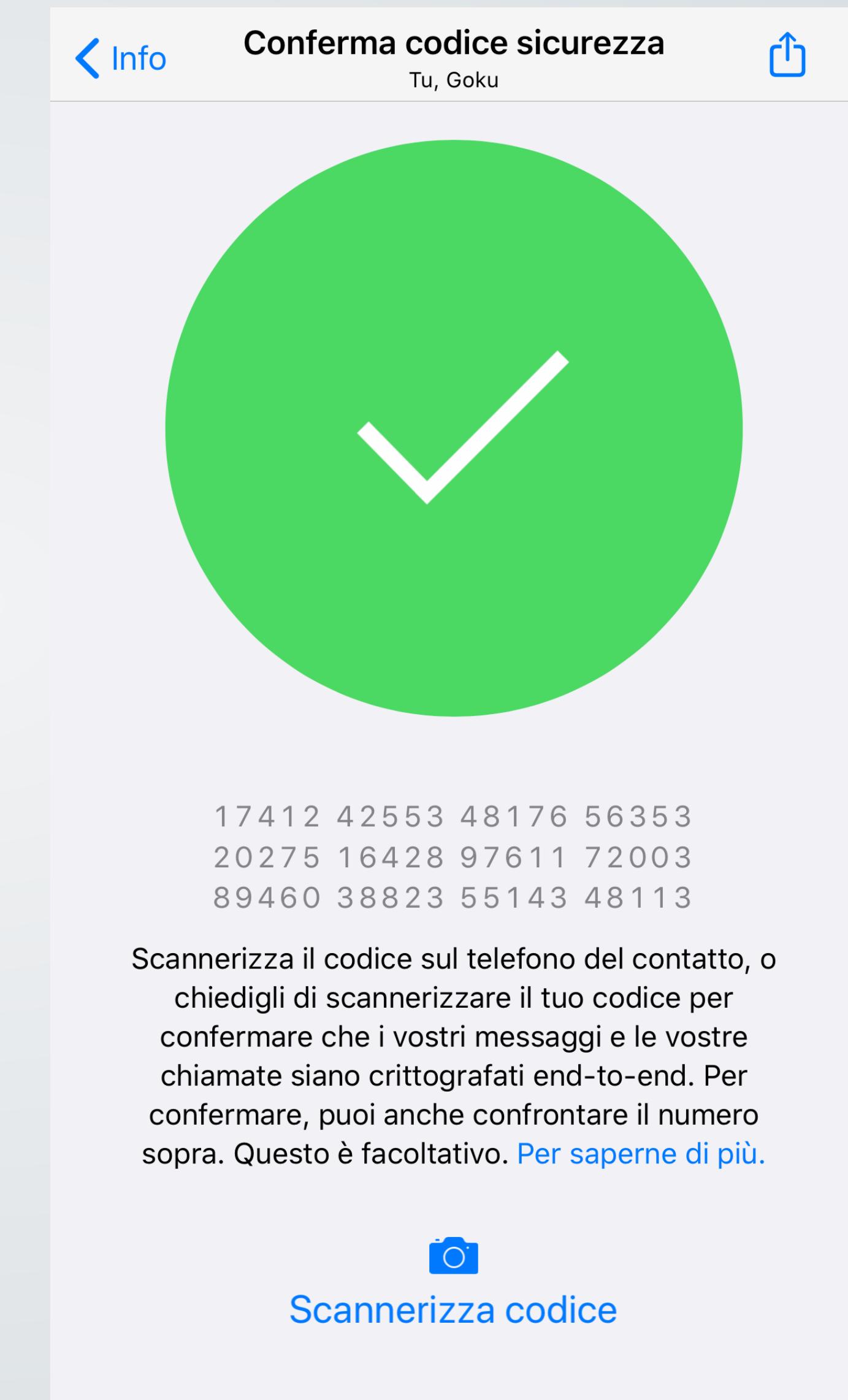
Contromisure: WhatsApp



Contromisure: WhatsApp



Contromisure: WhatsApp



Quindi nel mondo reale si usa DH?



Telegram Voice Call authentication

"Keys for end-to-end encrypted calls are generated using the Diffie-Hellman key exchange. Users who are on a call can ensure that there is no MitM by comparing key visualizations."



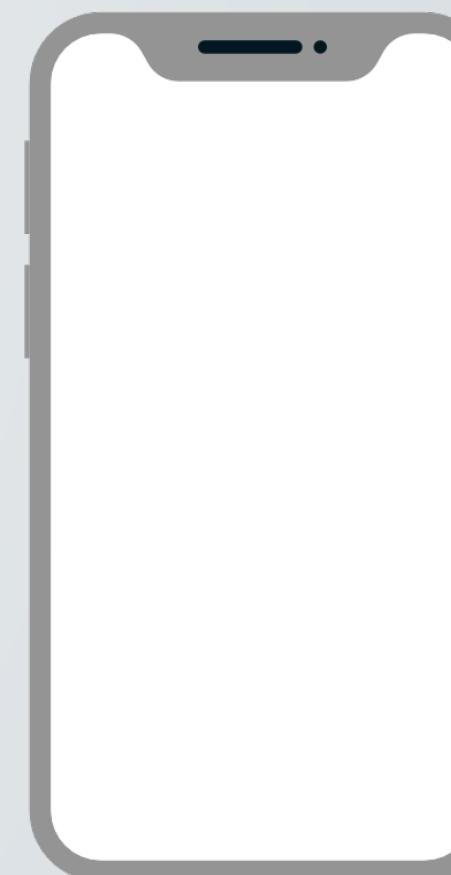
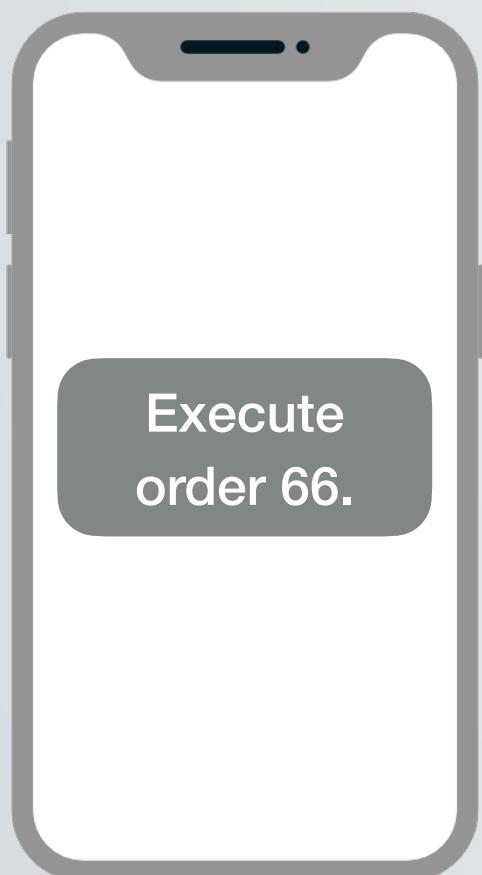
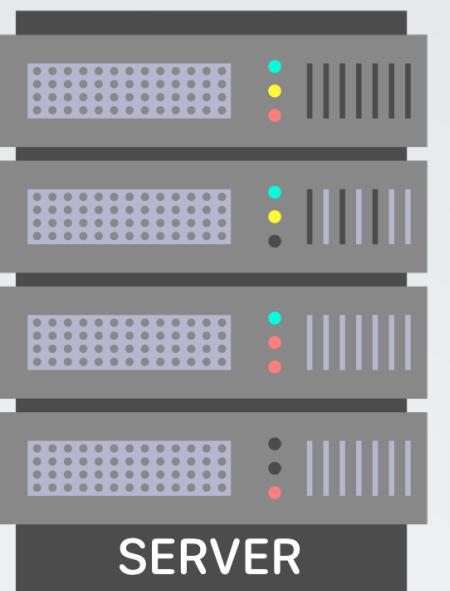
Signal key agreement protocol

"This document describes the "X3DH" (or "Extended Triple Diffie-Hellman") key agreement protocol. X3DH establishes a shared secret key between two parties who mutually authenticate each other based on public keys. X3DH provides forward secrecy and cryptographic deniability."

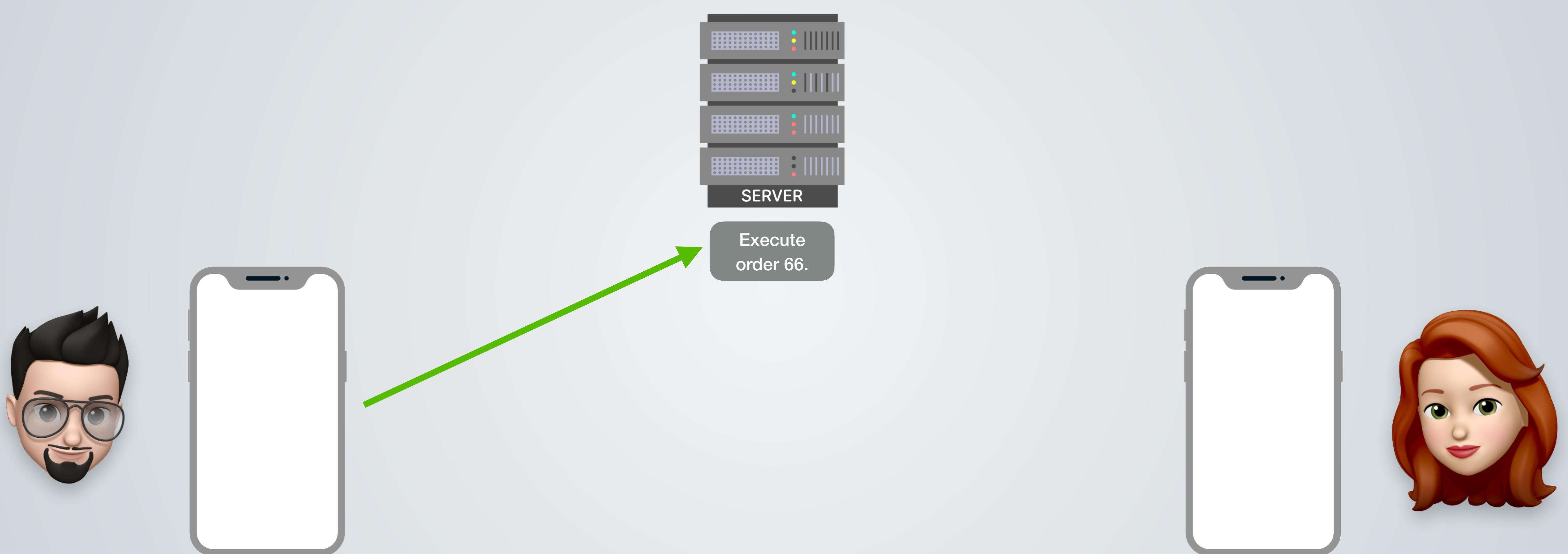


Crittografia
end-to-end

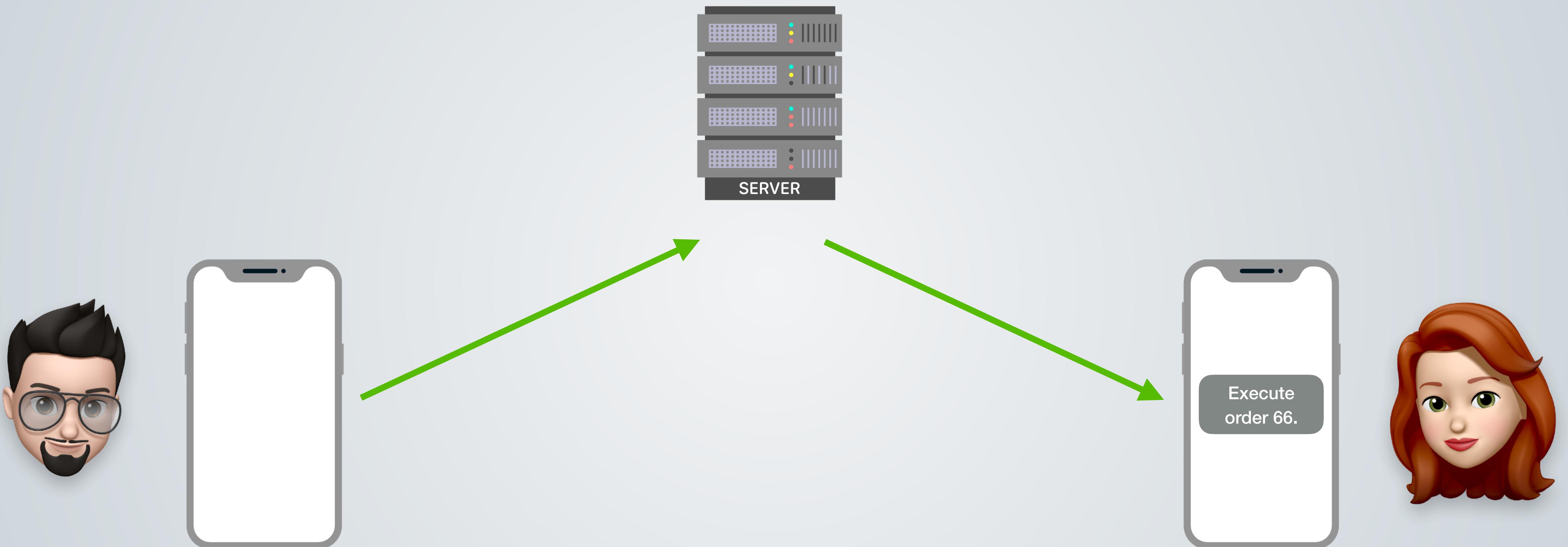
Instant messaging: plain text



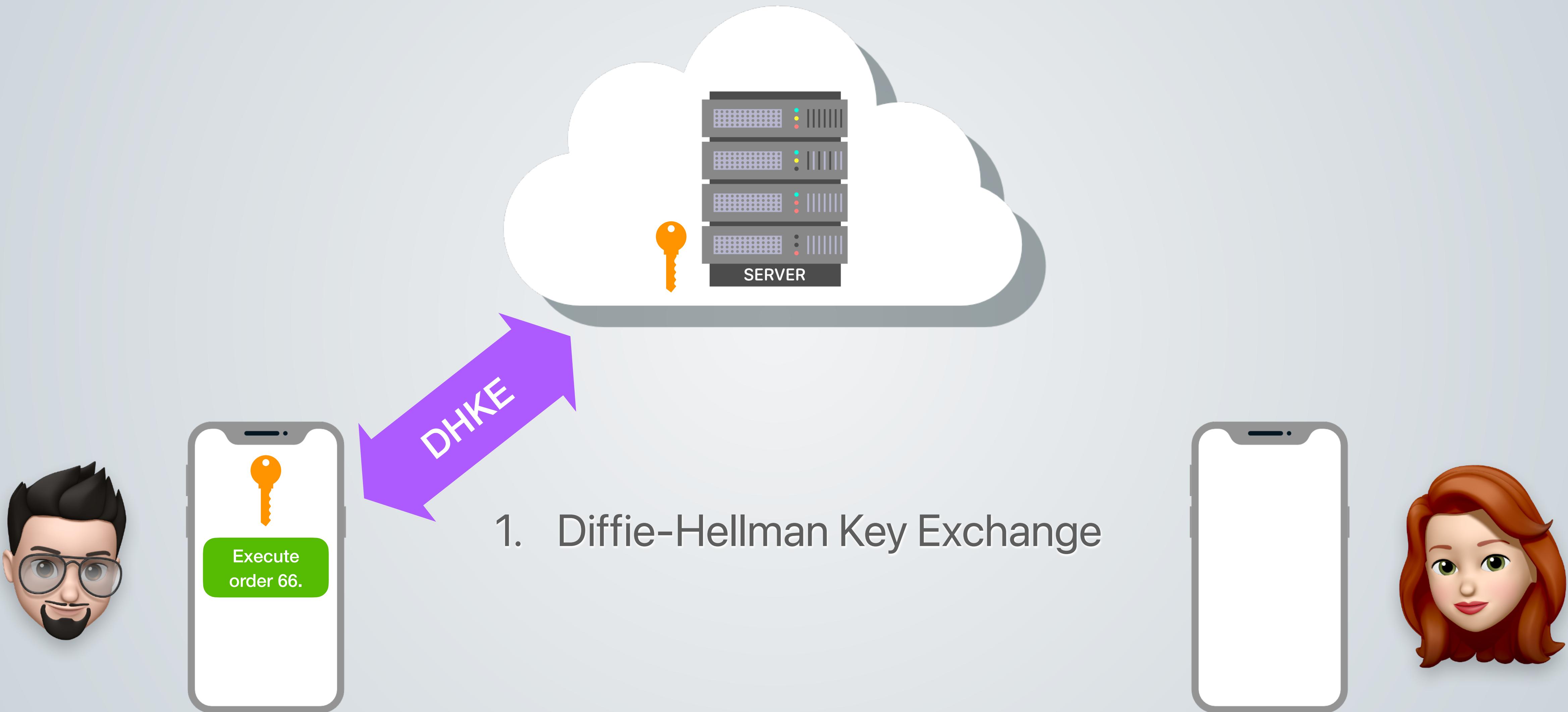
Instant messaging: plain text



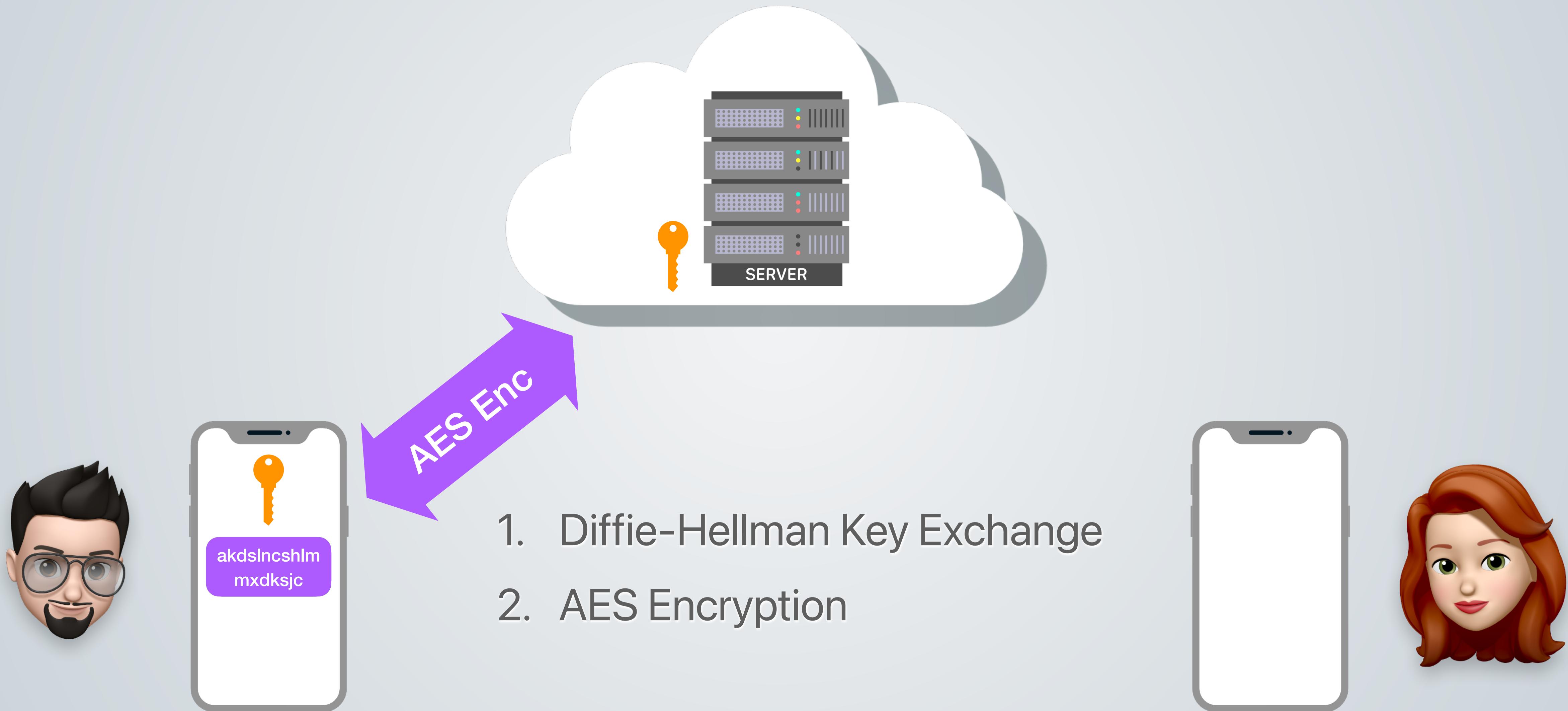
Instant messaging: plain text



Instant messaging: encryption



Instant messaging: encryption



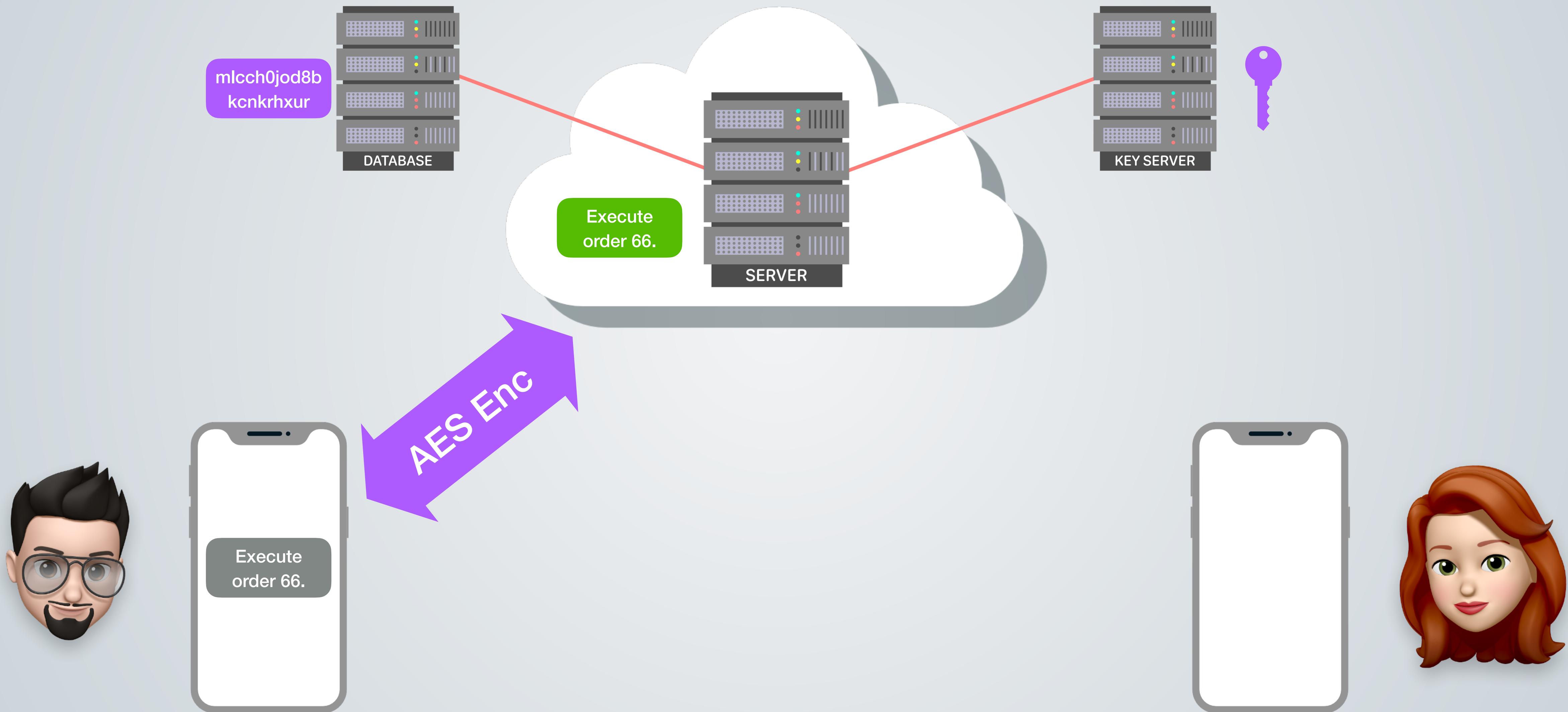
Instant messaging: encryption



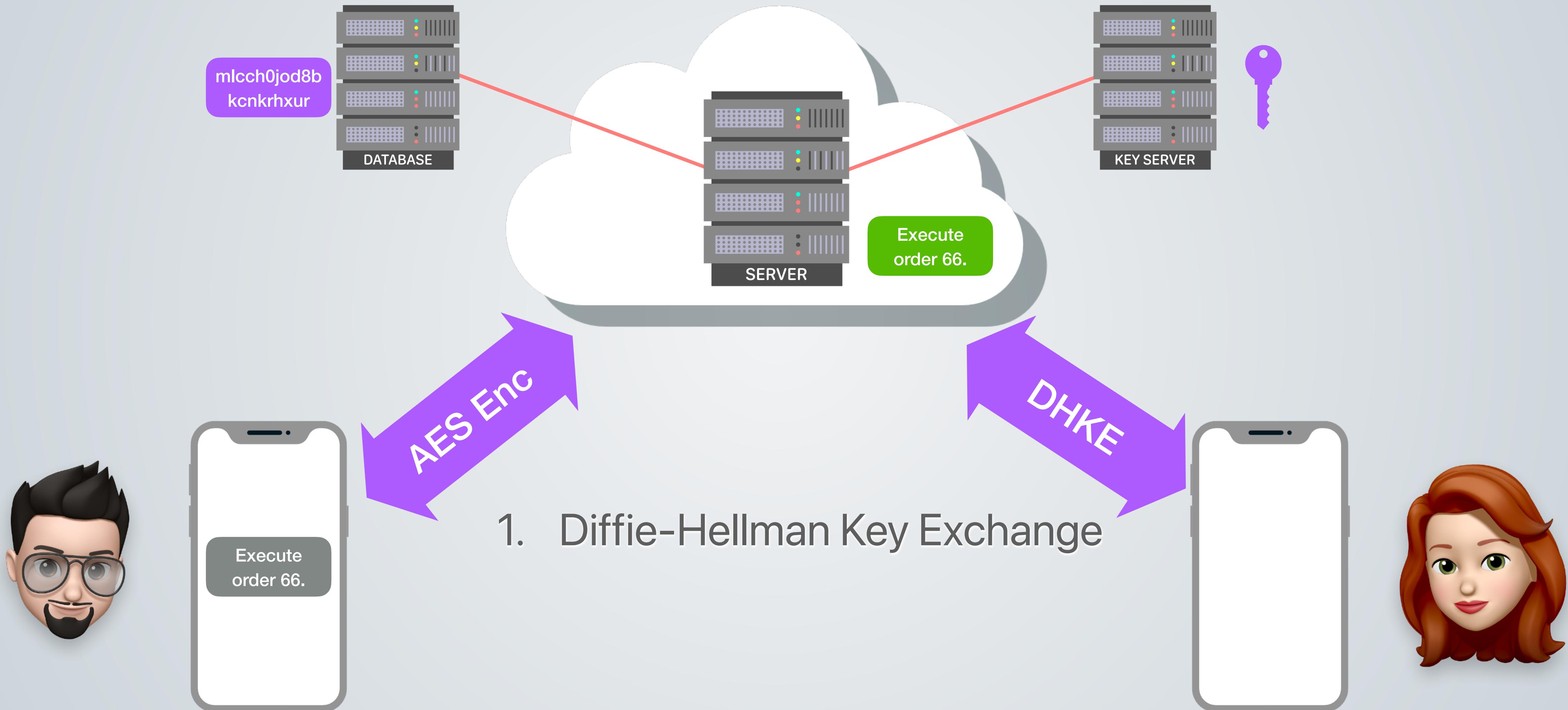
Instant messaging: encryption



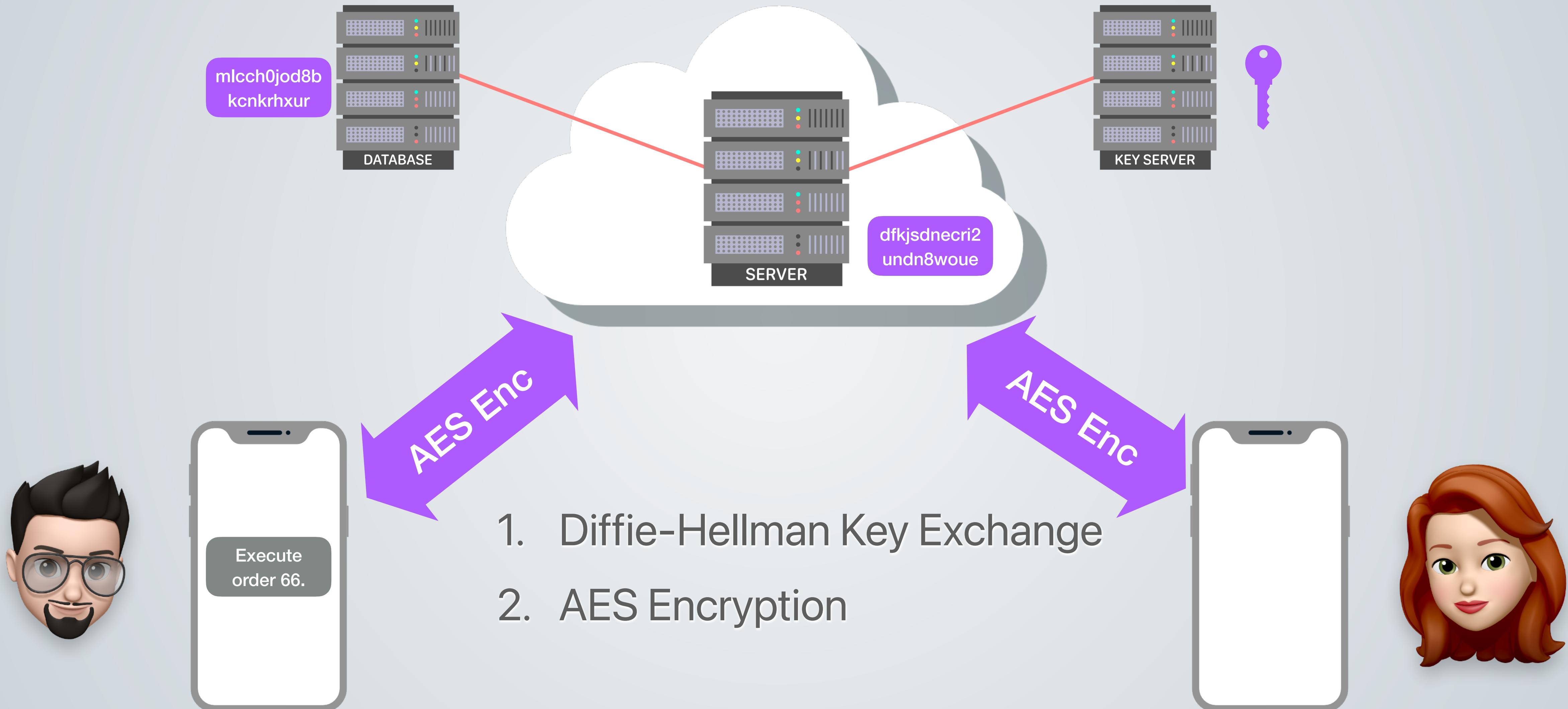
Instant messaging: encryption



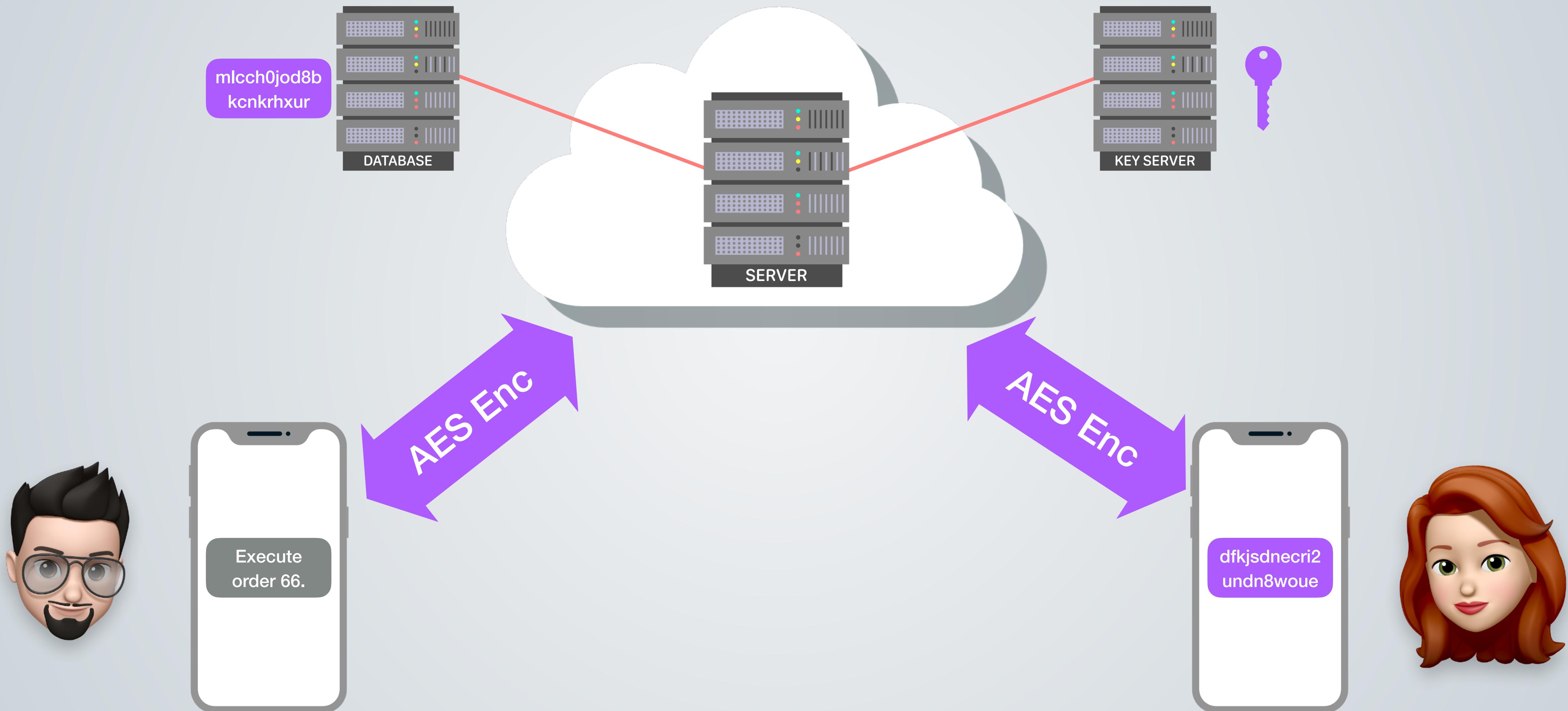
Instant messaging: encryption



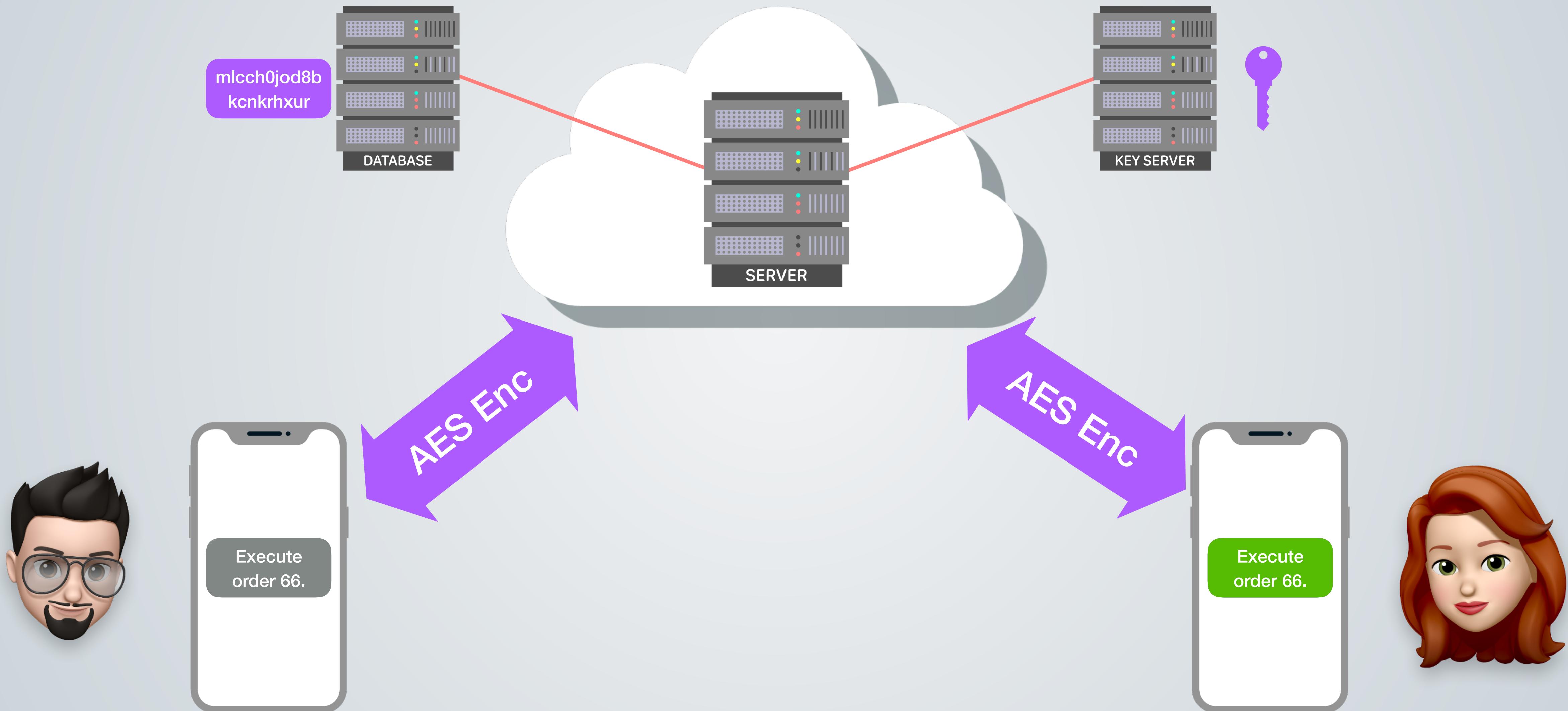
Instant messaging: encryption



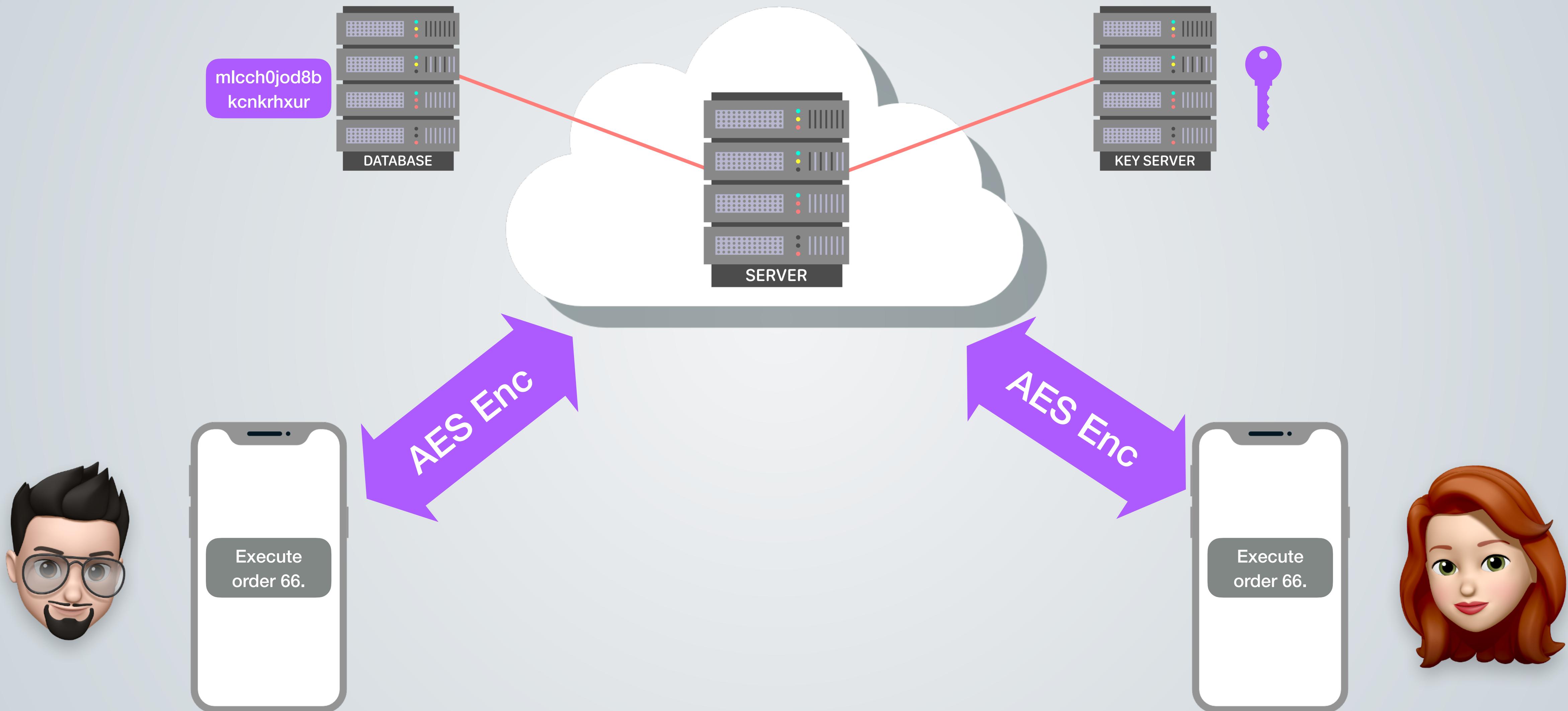
Instant messaging: encryption



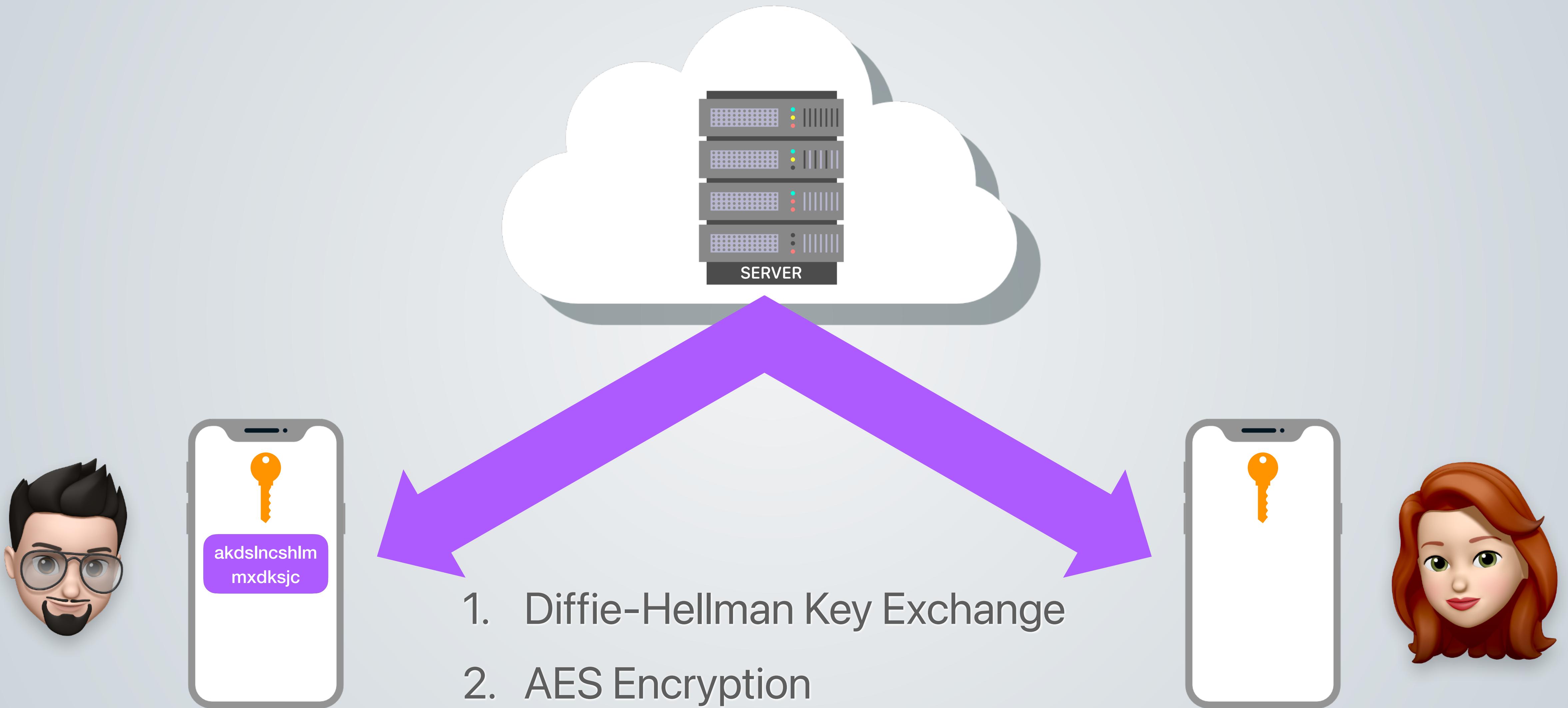
Instant messaging: encryption



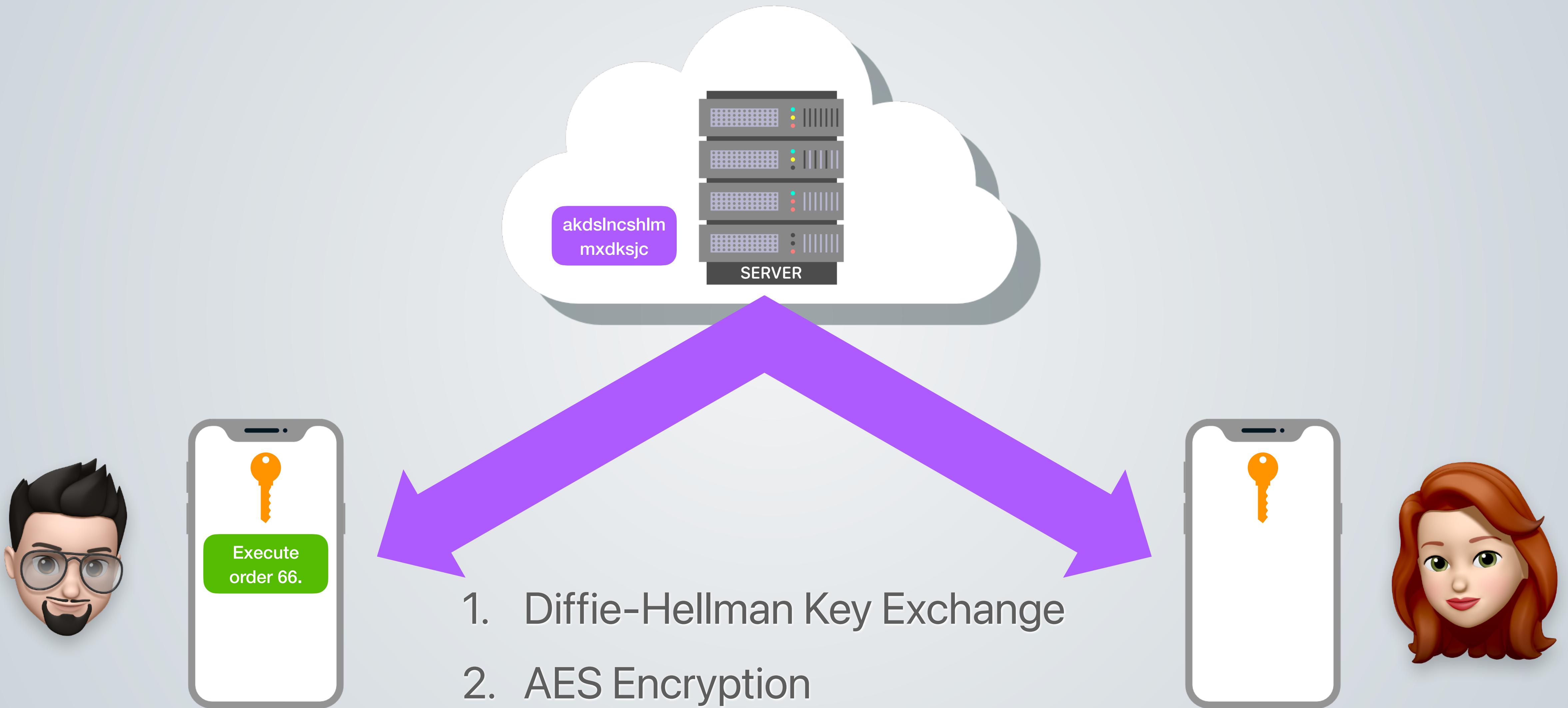
Instant messaging: encryption



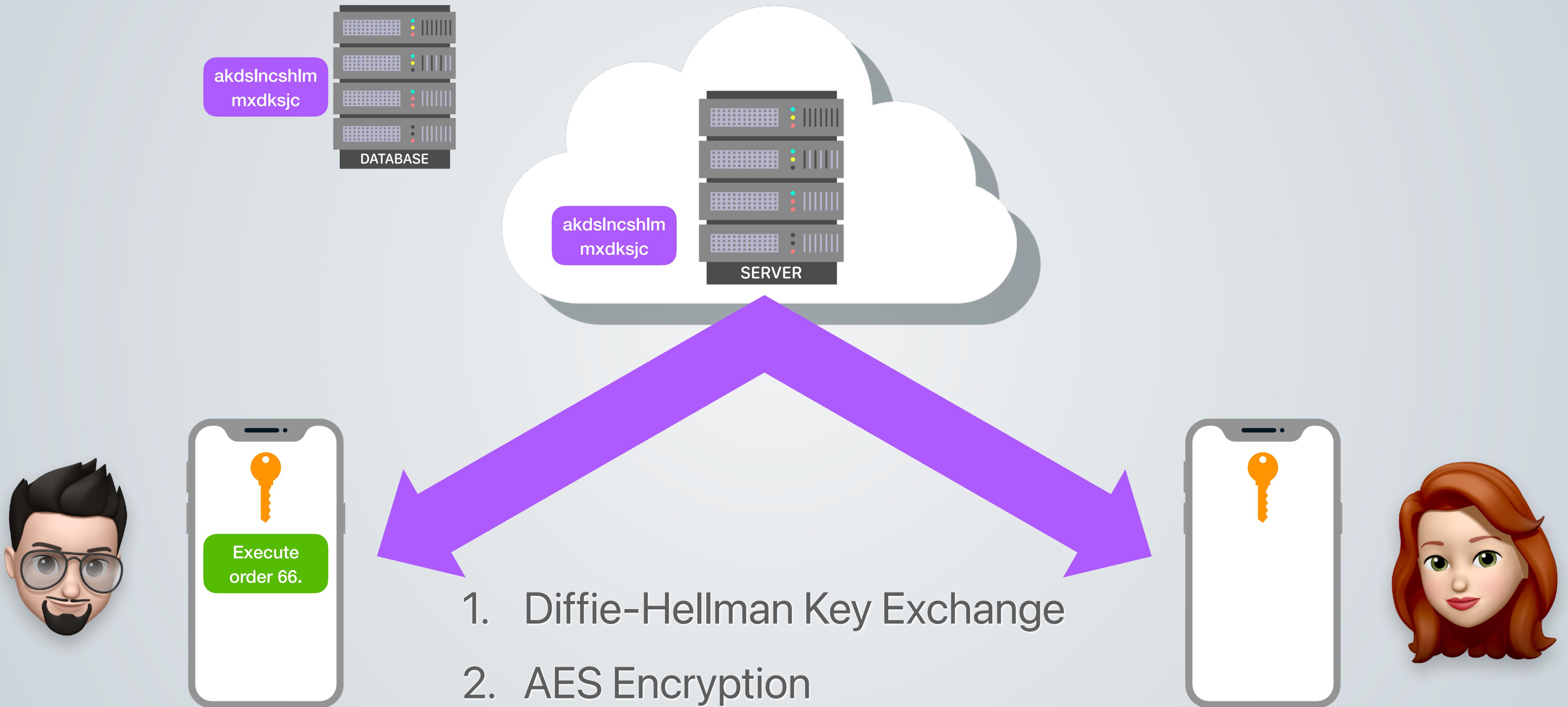
Instant messaging: end-to-end encryption



Instant messaging: end-to-end encryption



Instant messaging: end-to-end encryption



Instant messaging: end-to-end encryption

