COESIONE ITALIA 21-27 PIEMONTE
Cofinanziato dall'Unione europea
REGIONE PIEMONTE

WHATSAPP & TELEGRAM

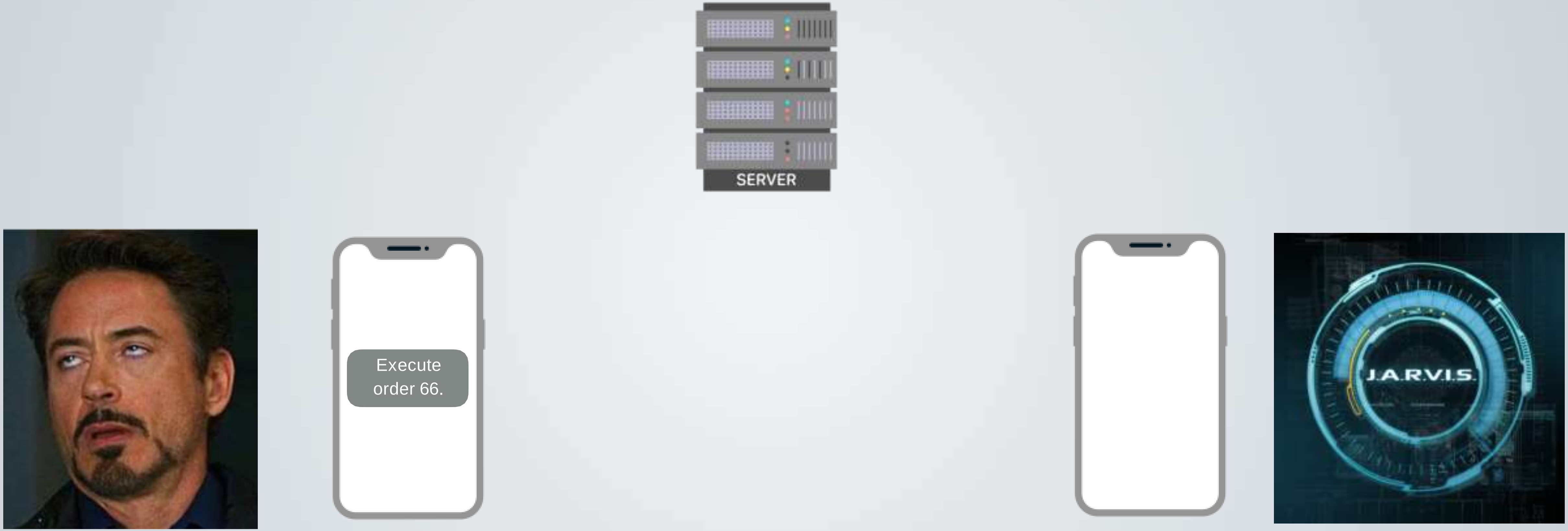
Sicurezza informatica

Elena Maria Dal Santo

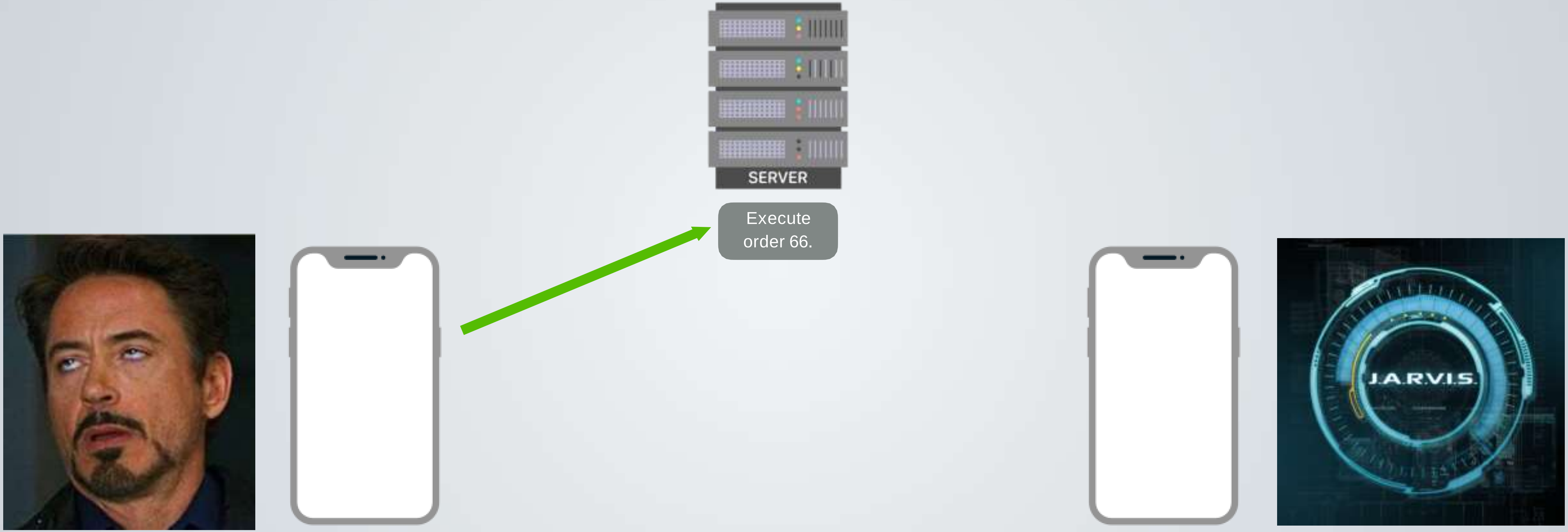
elenamaria.dalsanto@its-ictpiemonte.it

Intervento realizzato da
ITS
TECNOLOGIE
DELL'INFORMAZIONE E
DELLA COMUNICAZIONE

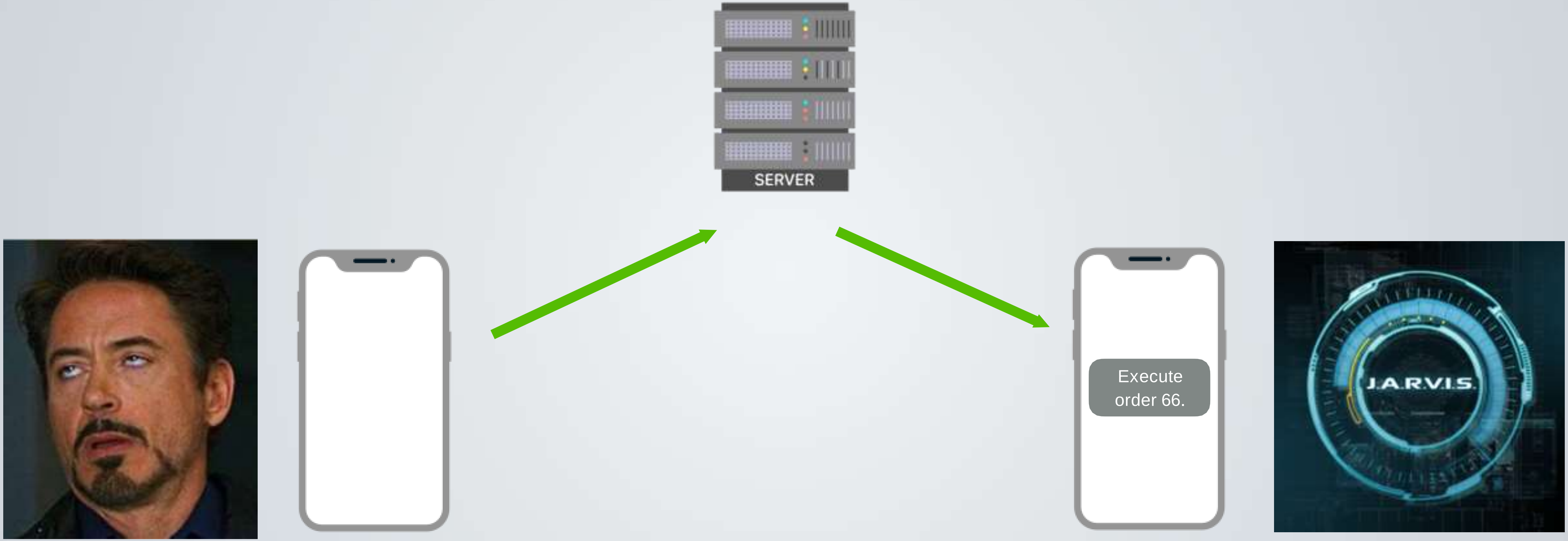
Instant messaging: plain text



Execute order 66.



Execute order 66.

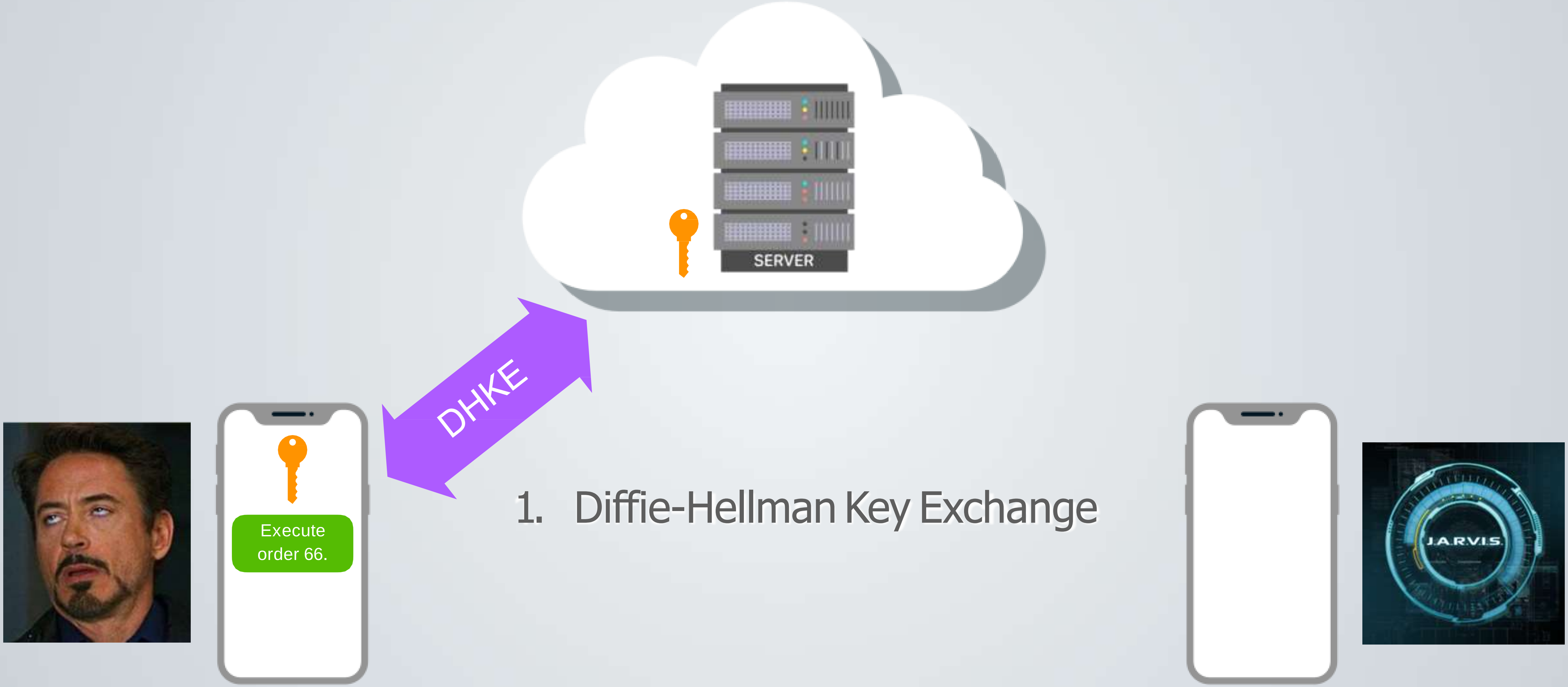


Execute order 66.

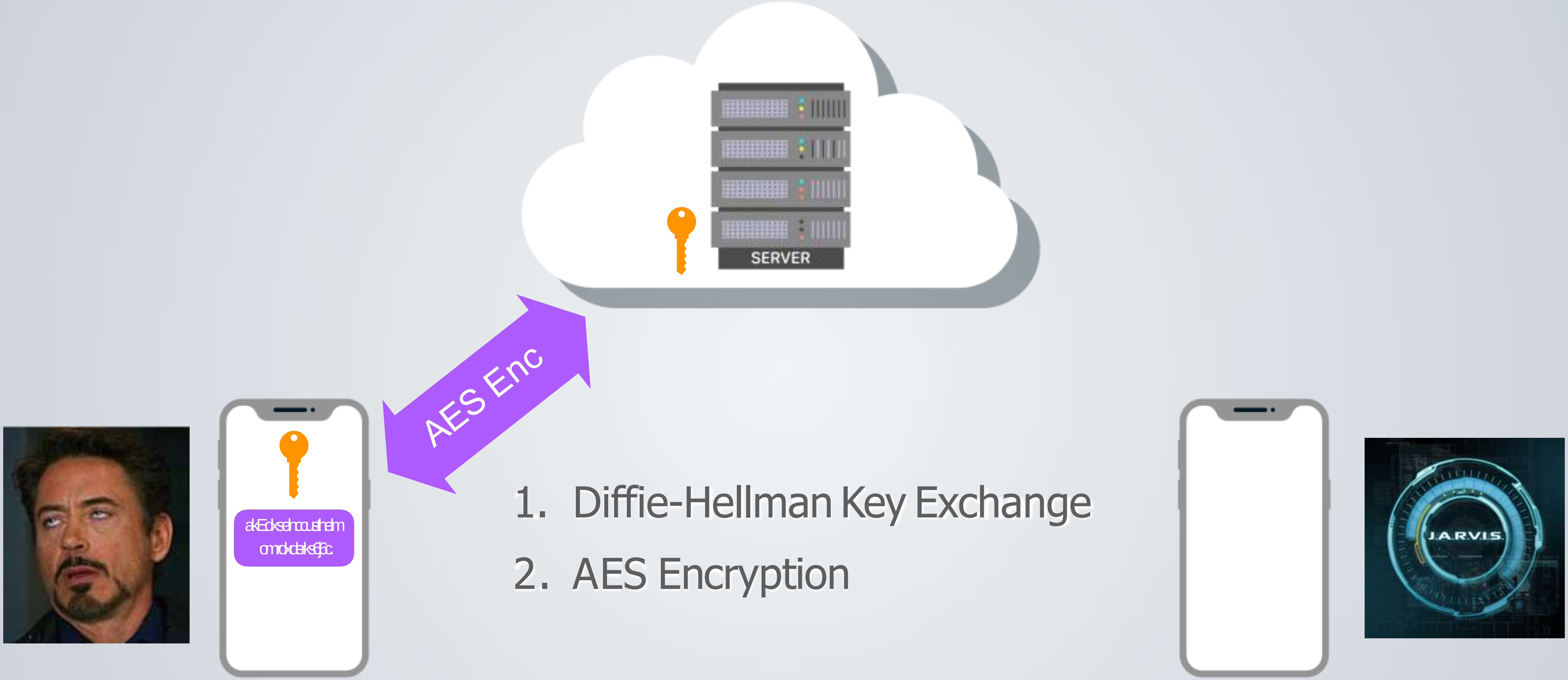
Questo è un caso base che presenta però evidenti problemi

1) I messaggi sono in chiaro
2) L’intermediario (server) legge e può quindi salvare questi messaggi in chiaro
3) Un eventuale attacco man-in-the-middle sarebbe fin troppo facile

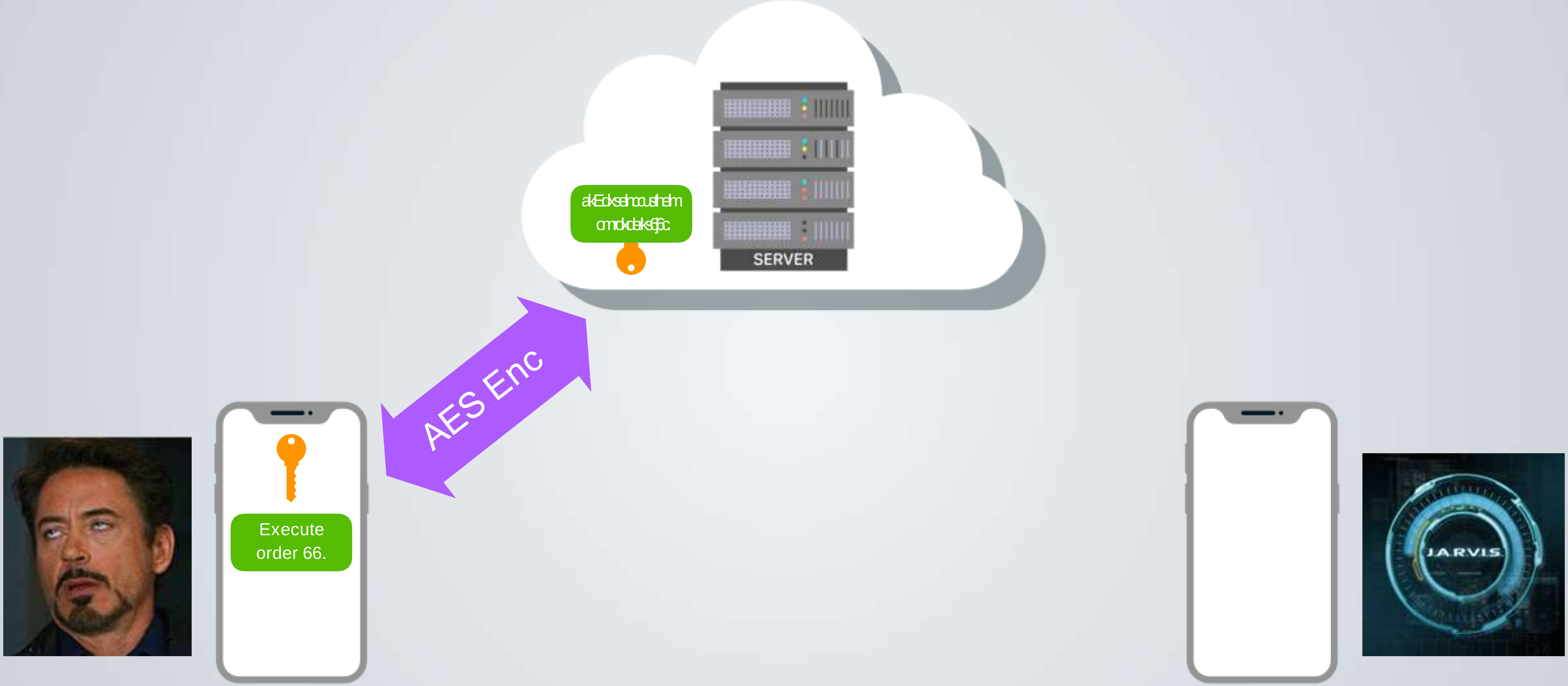
Instant messaging: encryption

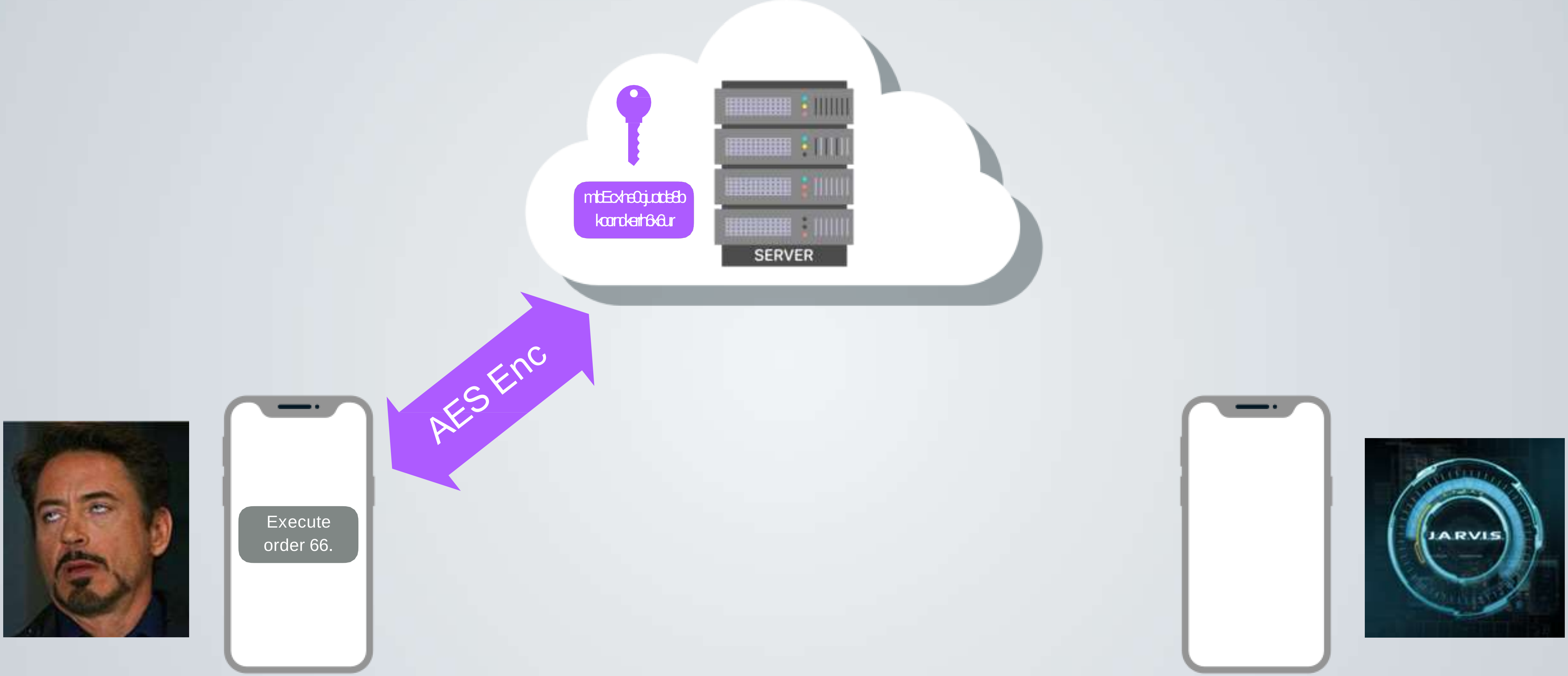


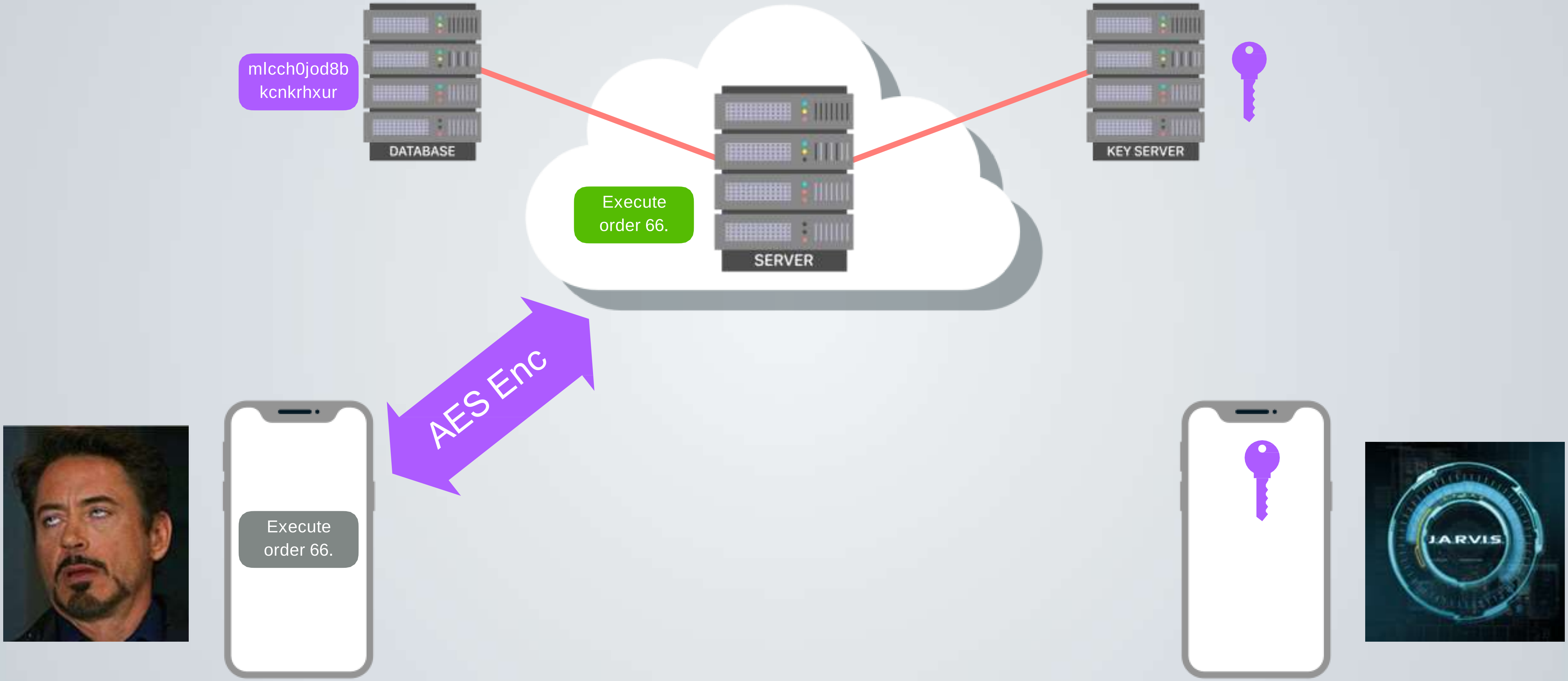
1. Diffie-Hellman Key Exchange



1. Diffie-Hellman Key Exchange
2. AES Encryption


akEdxsehcousthelm
omrdxdarks6j6c.
SERVER
AES Enc
Execute
order 66.
J.A.R.V.I.S.


mlbEcxhe0gjuotde8b
kcoarndkerh6x6ur
SERVER
AES Enc
Execute
order 66.
J.A.R.V.I.S.



mlcch0jod8b
kcnkrhxur

DATABASE

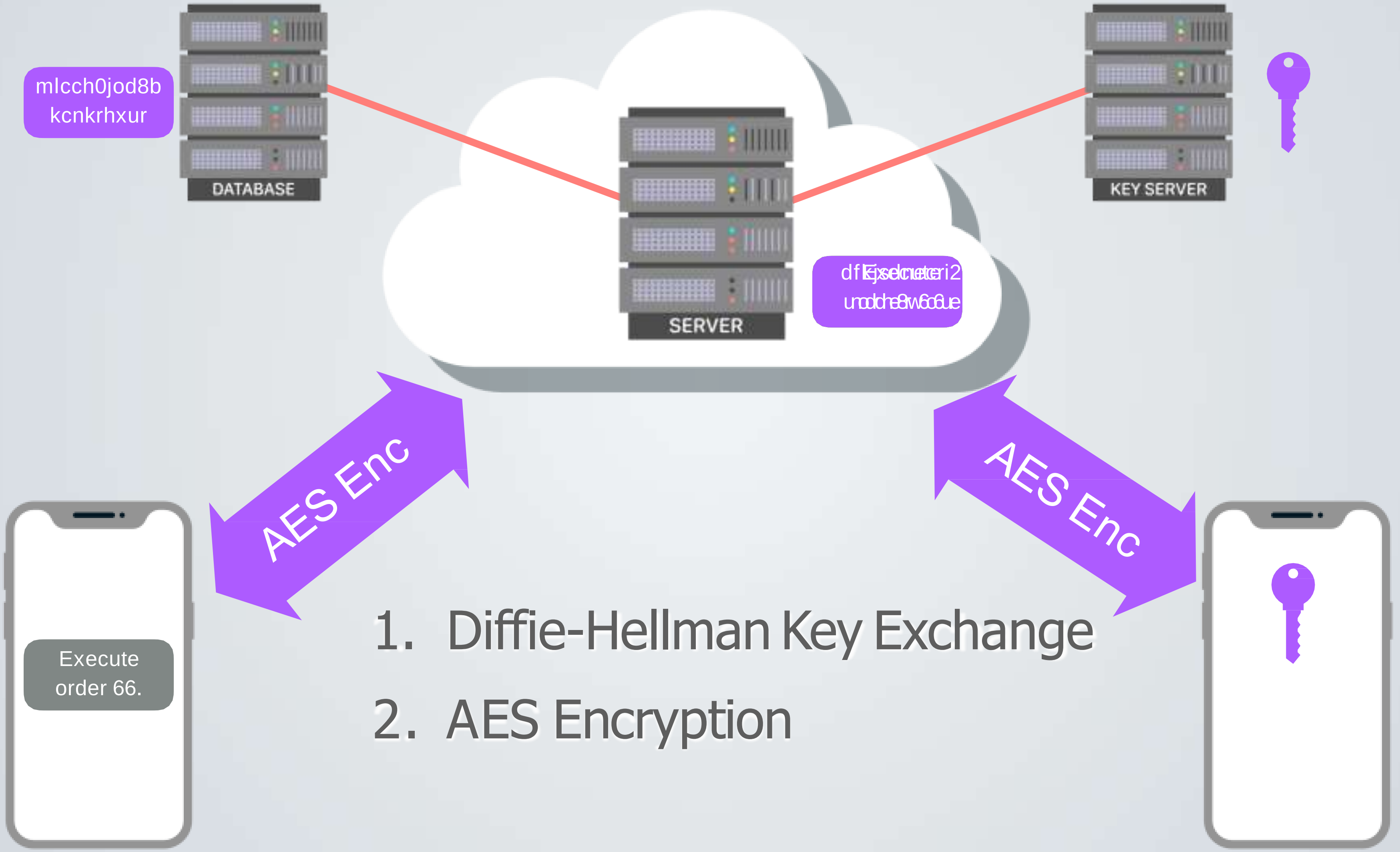
Execute
order 66.

SERVER

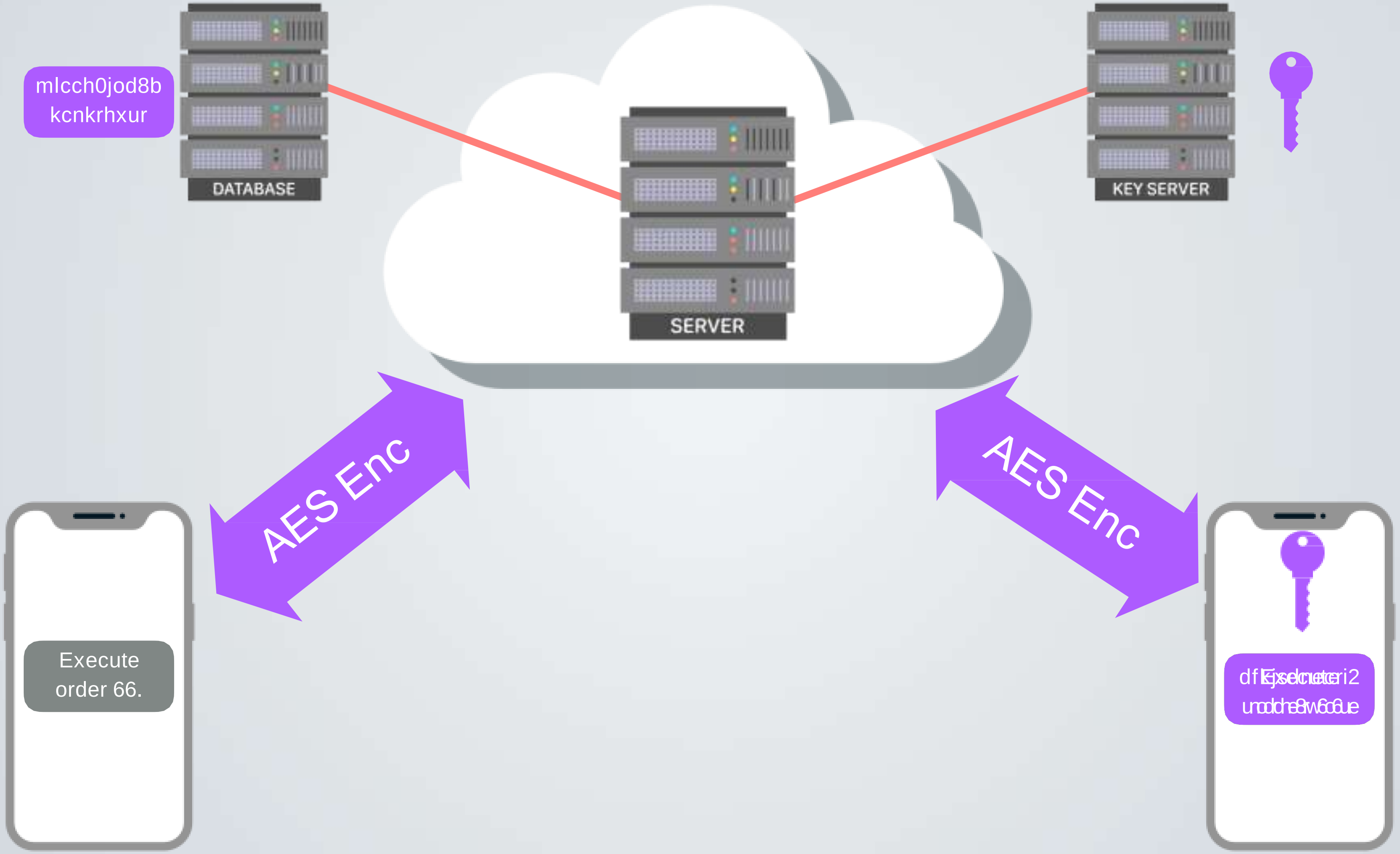
KEY SERVER

AES Enc

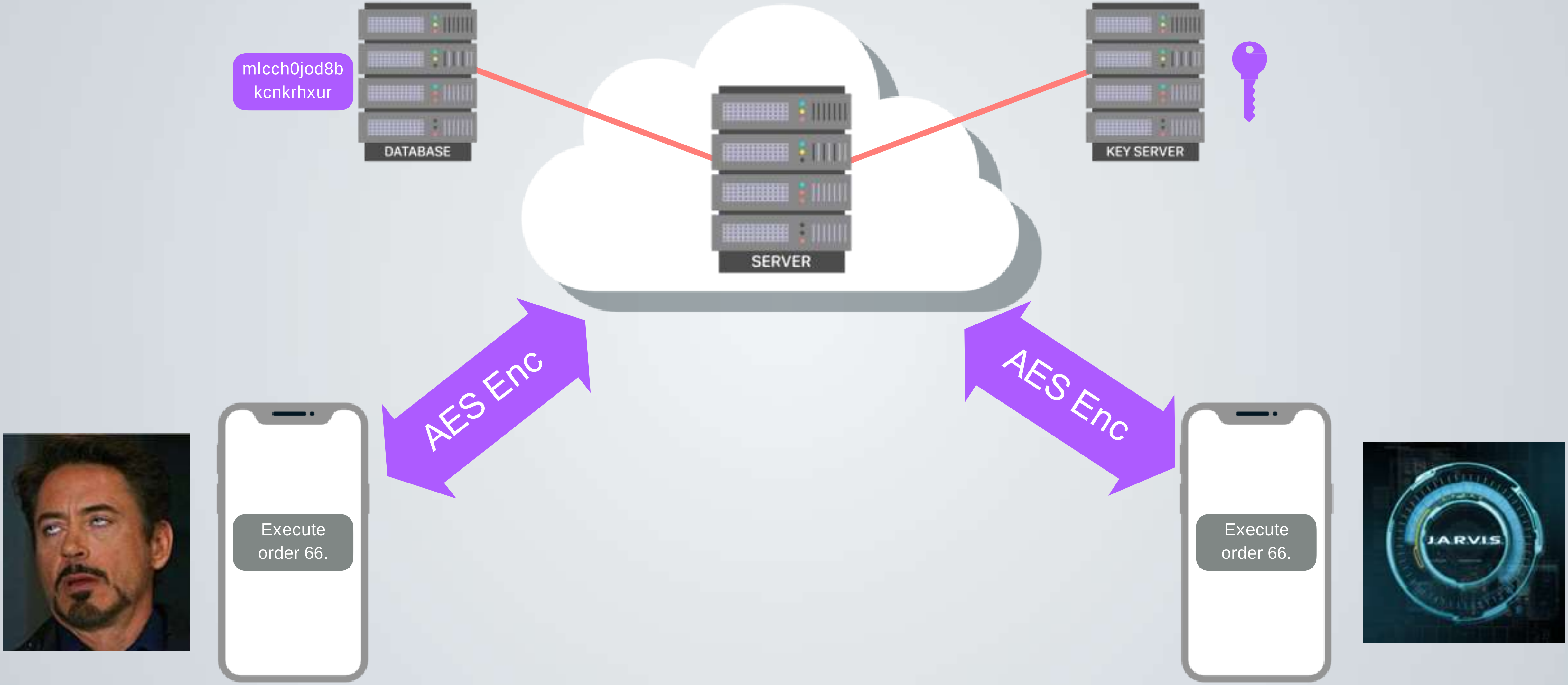
Execute
order 66.



1. Diffie-Hellman Key Exchange
2. AES Encryption


mlcch0jod8b
kcnkrhxur
DATABASE
SERVER
KEY SERVER
AES Enc
AES Enc
Execute
order 66.
dfkEjxselcnueteri2
unoclche8w6o6ue

J.A.R.V.I.S.


mlcch0jod8b
kcnkrhxur
DATABASE
SERVER
KEY SERVER
AES Enc
AES Enc
Execute order 66.
Execute order 66.
J.A.R.V.I.S.

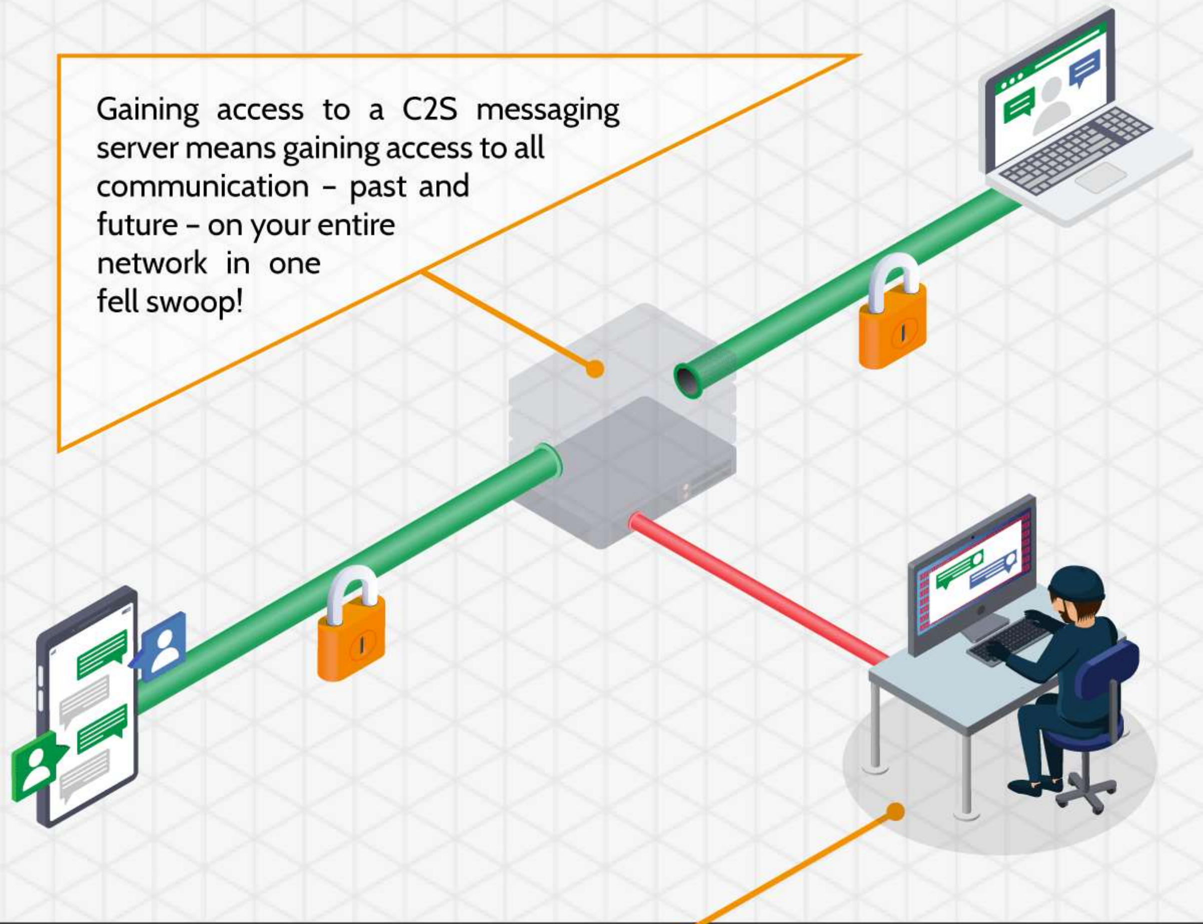
I messaggi sono ora nascosti, però…

~~1)I messaggi sono in chiaro~~

2)L’intermediario (server) legge e può quindi salvare questi messaggi perché ha la chiave

3)Un eventuale attacco man-in-the-middle sarebbe fin troppo facile (potrebbero addirittura intercettare un testo in chiaro lato server!)

CLIENT-TO-SERVER ENCRYPTION

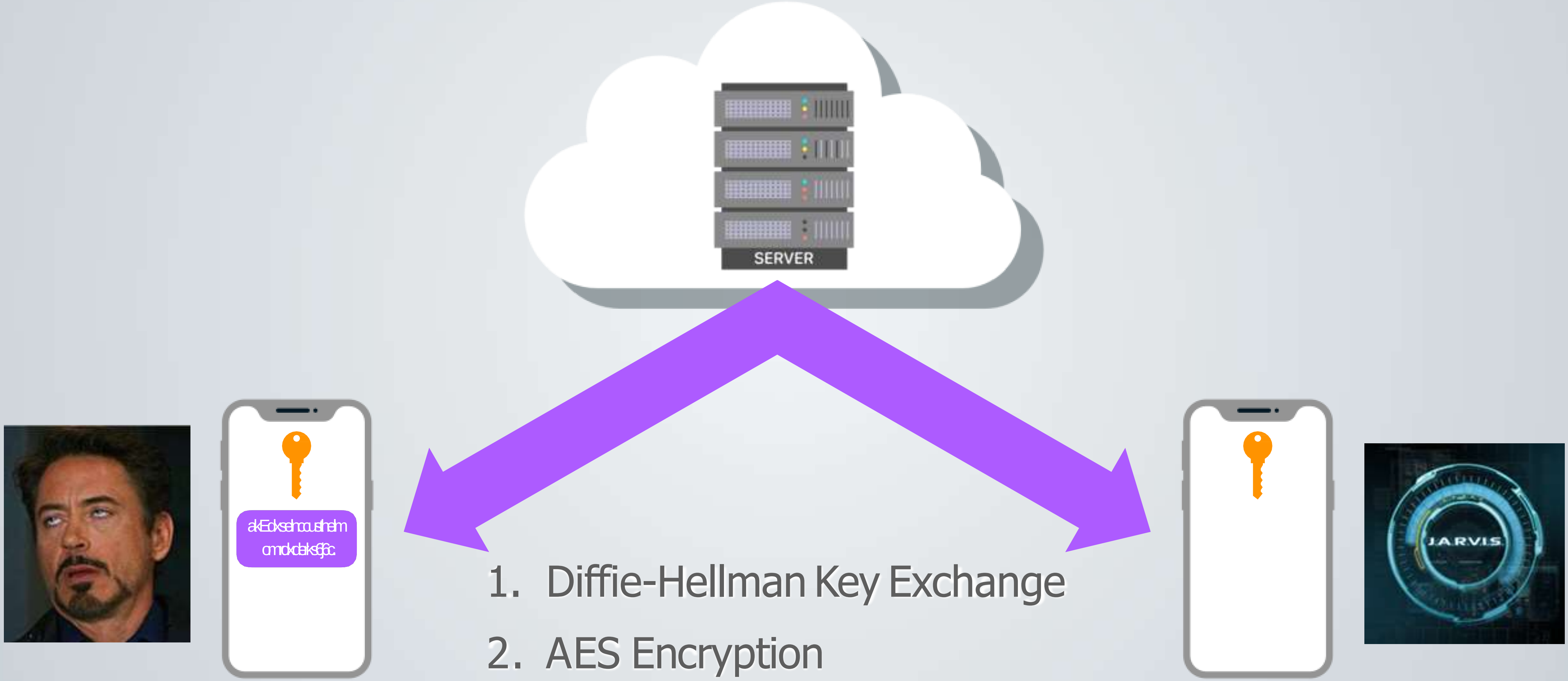


Gaining access to a C2S messaging server means gaining access to all communication – past and future – on your entire network in one fell swoop!

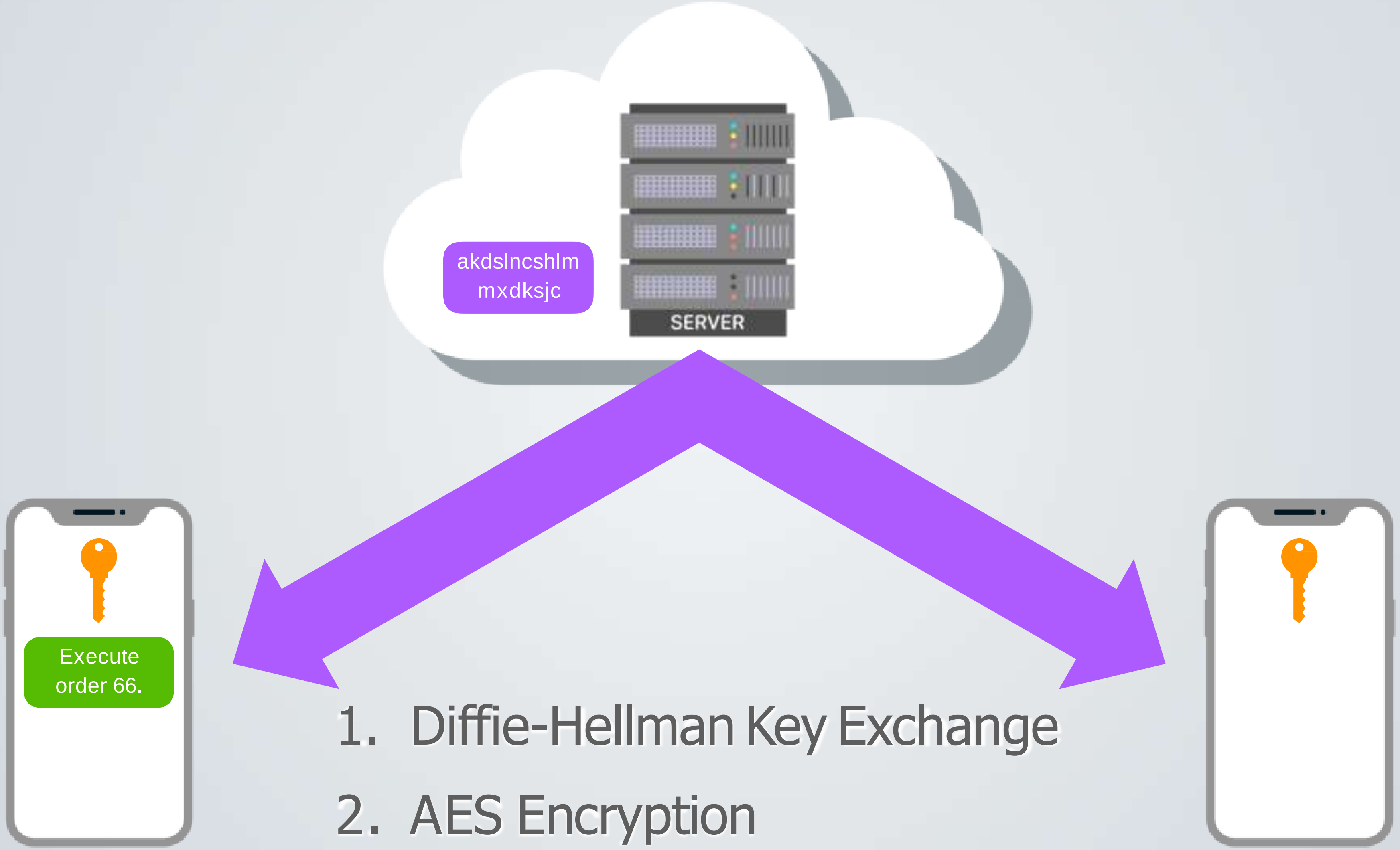
Not Just Hackers

Insider attacks are, by far, the most dominant type of threat to the cybersecurity of organizations.

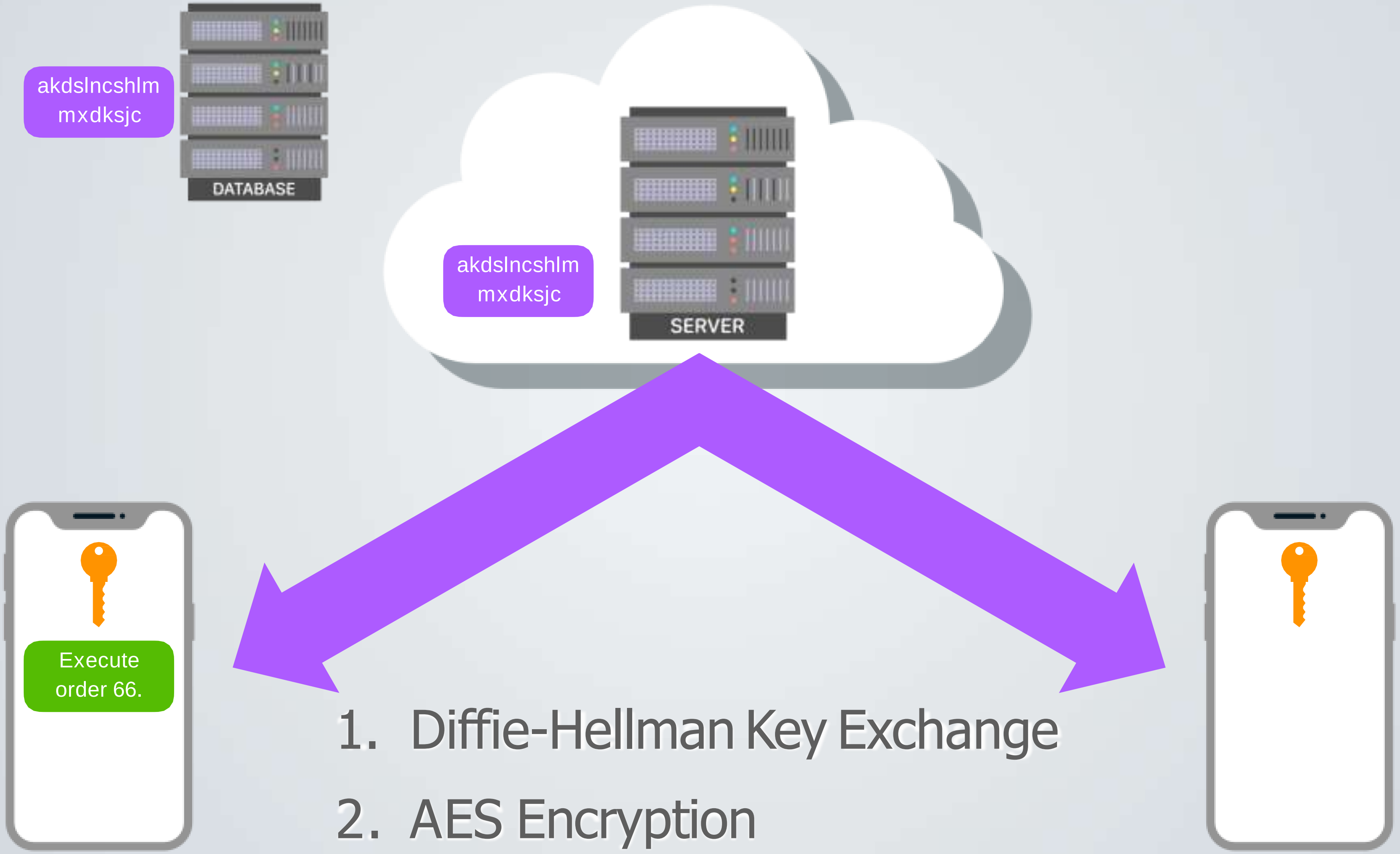
Instant messaging: end-to-end encryption



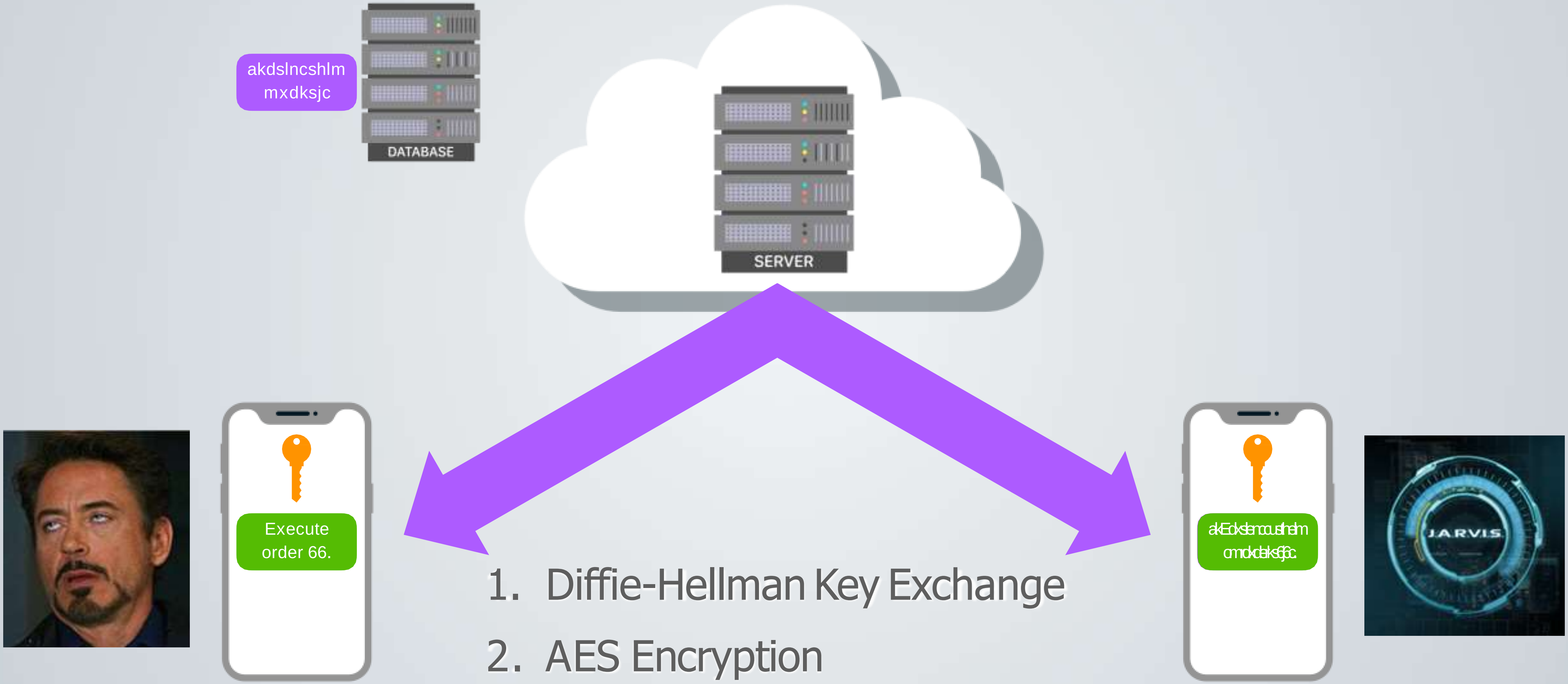
1. Diffie-Hellman Key Exchange
2. AES Encryption



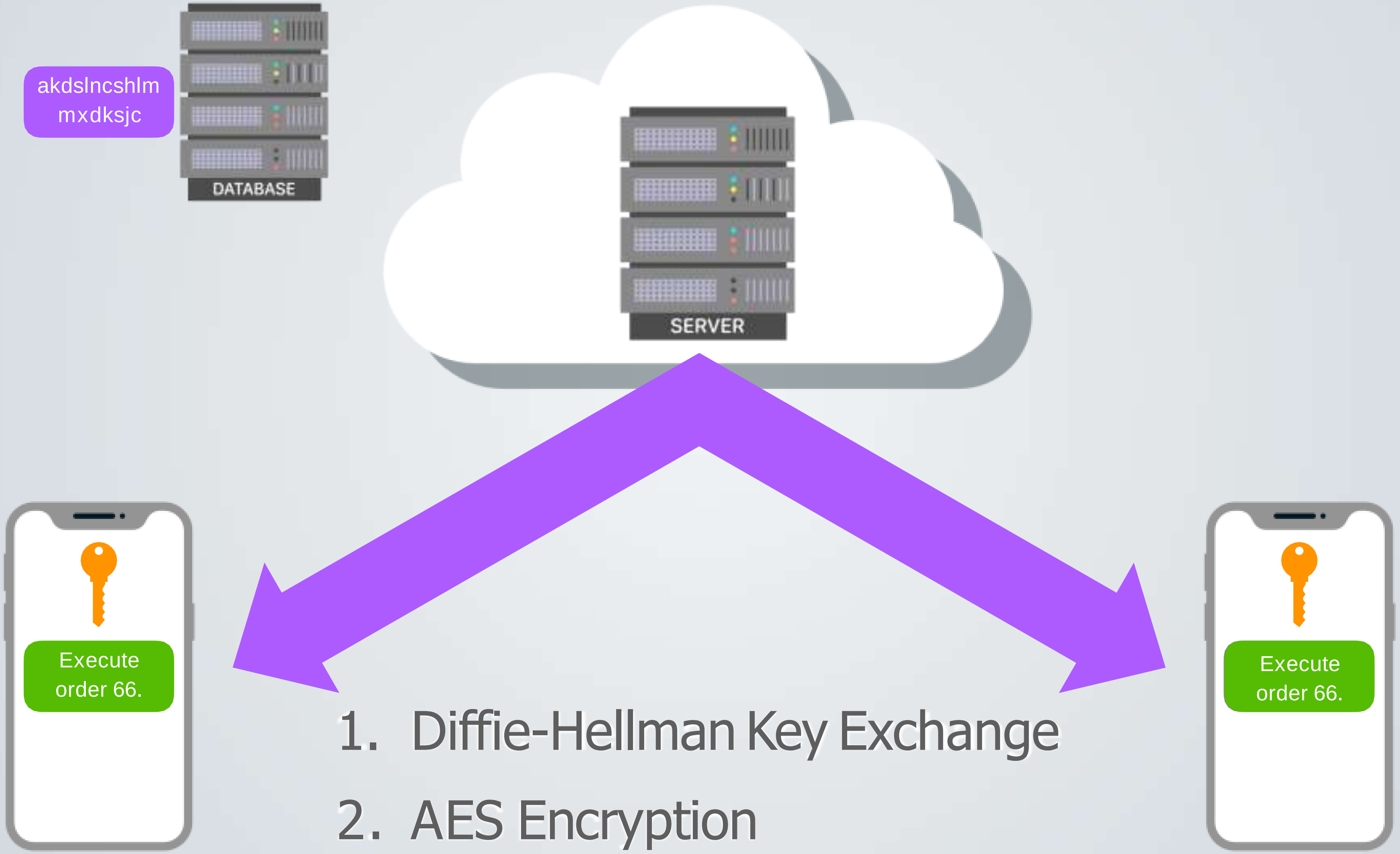
1. Diffie-Hellman Key Exchange
2. AES Encryption



1. Diffie-Hellman Key Exchange
2. AES Encryption



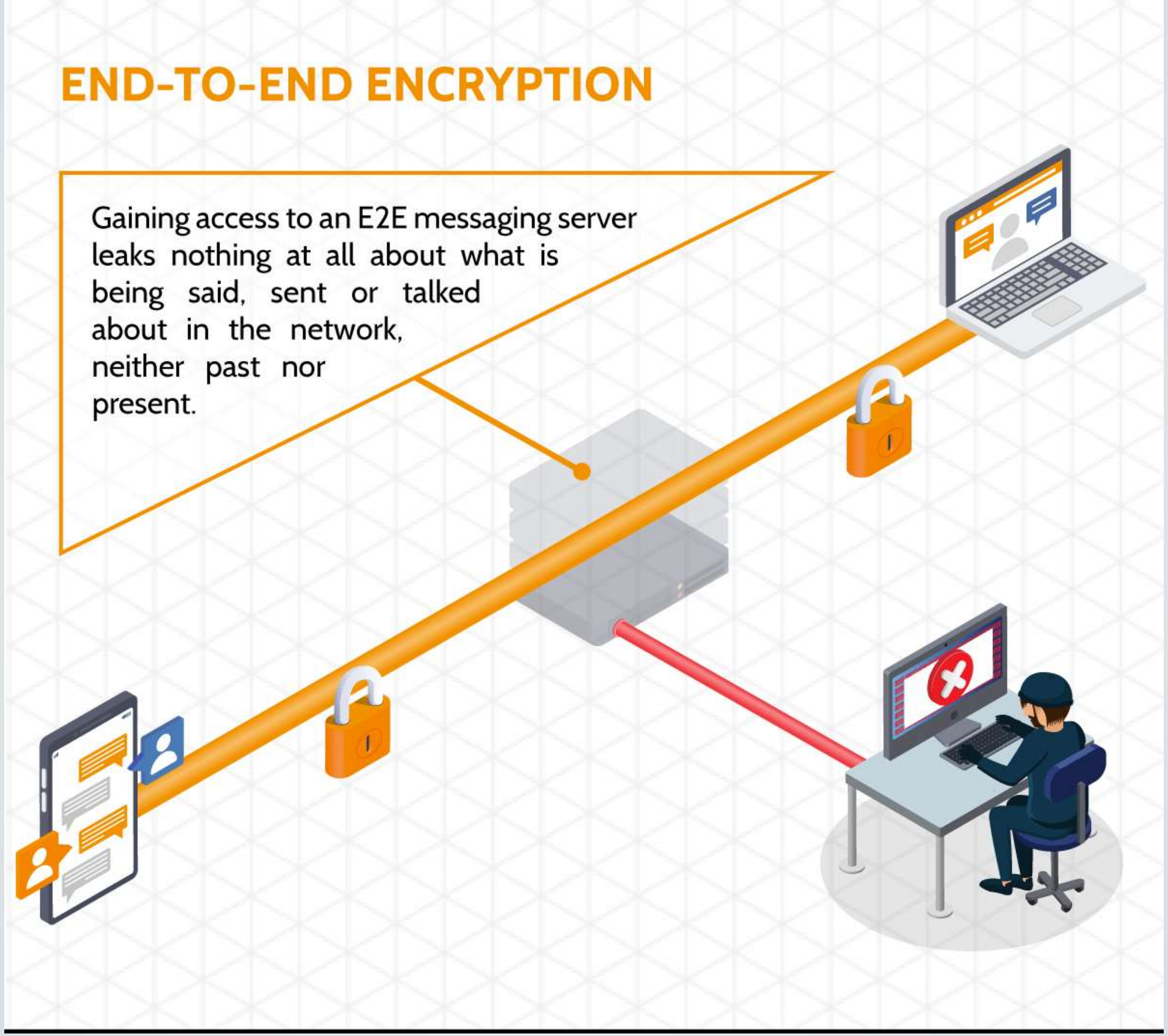
1. Diffie-Hellman Key Exchange
2. AES Encryption



1. Diffie-Hellman Key Exchange
2. AES Encryption

La crittografia end-to-end è un sistema di comunicazione cifrata in cui solo gli interlocutori possono leggere i messaggi.

Agli intermediari tra i due non è consentito l’accesso alle chiavi di cifratura.



END-TO-END ENCRYPTION

Gaining access to an E2E messaging server leaks nothing at all about what is being said, sent or talked about in the network, neither past nor present.

Telegram

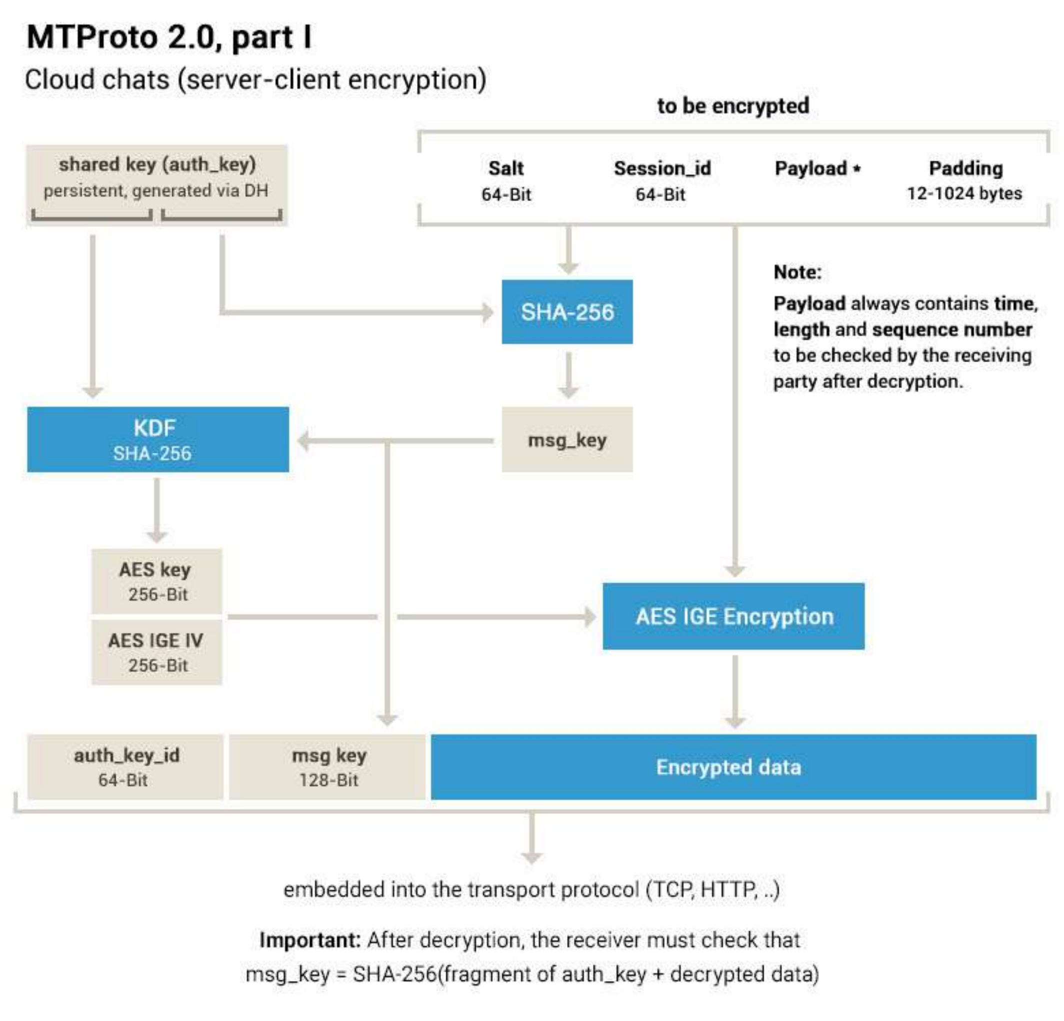
Novembre 2013: l’appena nato Telegram offre già chat con crittografia end-to-end

Oggi, Telegram usa:

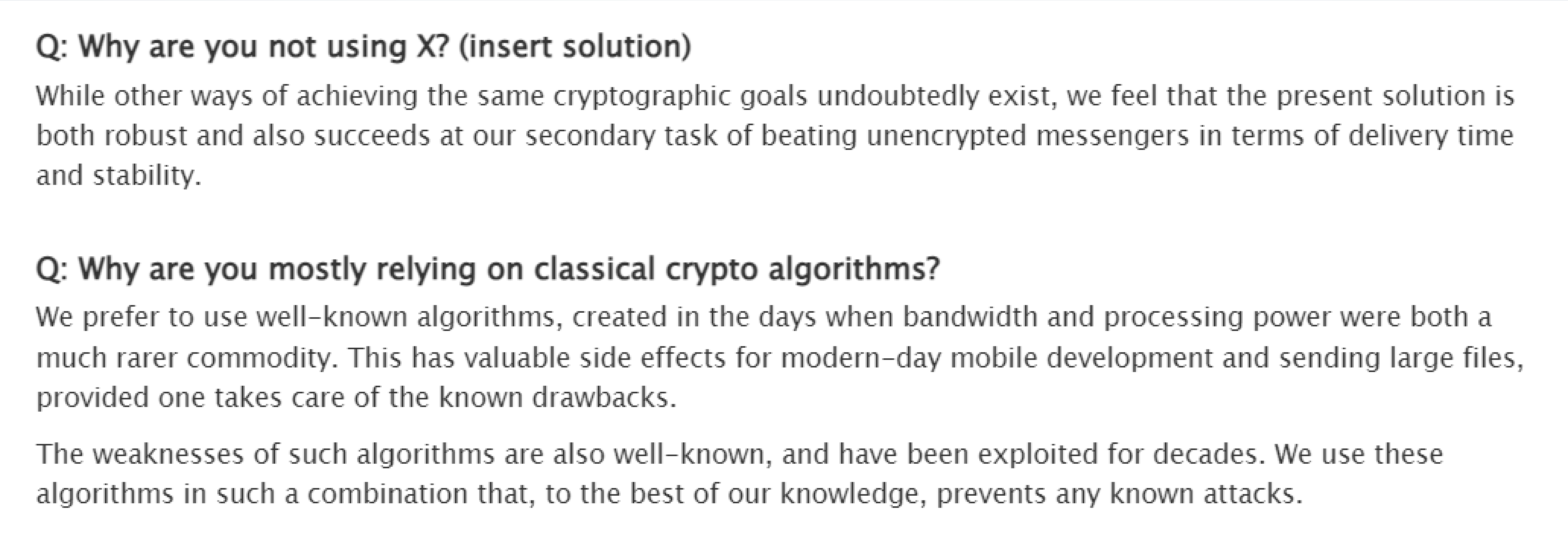
- Crittografia end-to-end per chat segrete
- Crittografia client-server per le chat ‘’normali’’

Telegram

Viene utilizzato un algoritmo chiamato MTProto, che supporta sia crittografia end-to-end che crittografia client-server


MTProto 2.0, part I
Cloud chats (server-client encryption)
to be encrypted
shared key (auth_key)
persistent, generated via DH
Salt
64-Bit
Session_id
64-Bit
Payload *
Padding
12-1024 bytes
SHA-256
Note:
Payload always contains time, length and sequence number to be checked by the receiving party after decryption.
KDF
SHA-256
msg_key
AES key
256-Bit
AES IGE IV
256-Bit
AES IGE Encryption
auth_key_id
64-Bit
msg key
128-Bit
Encrypted data
embedded into the transport protocol (TCP, HTTP, ..)
Important: After decryption, the receiver must check that
msg_key = SHA-256(fragment of auth_key + decrypted data)

Telegram



Q: Why are you not using X? (insert solution)

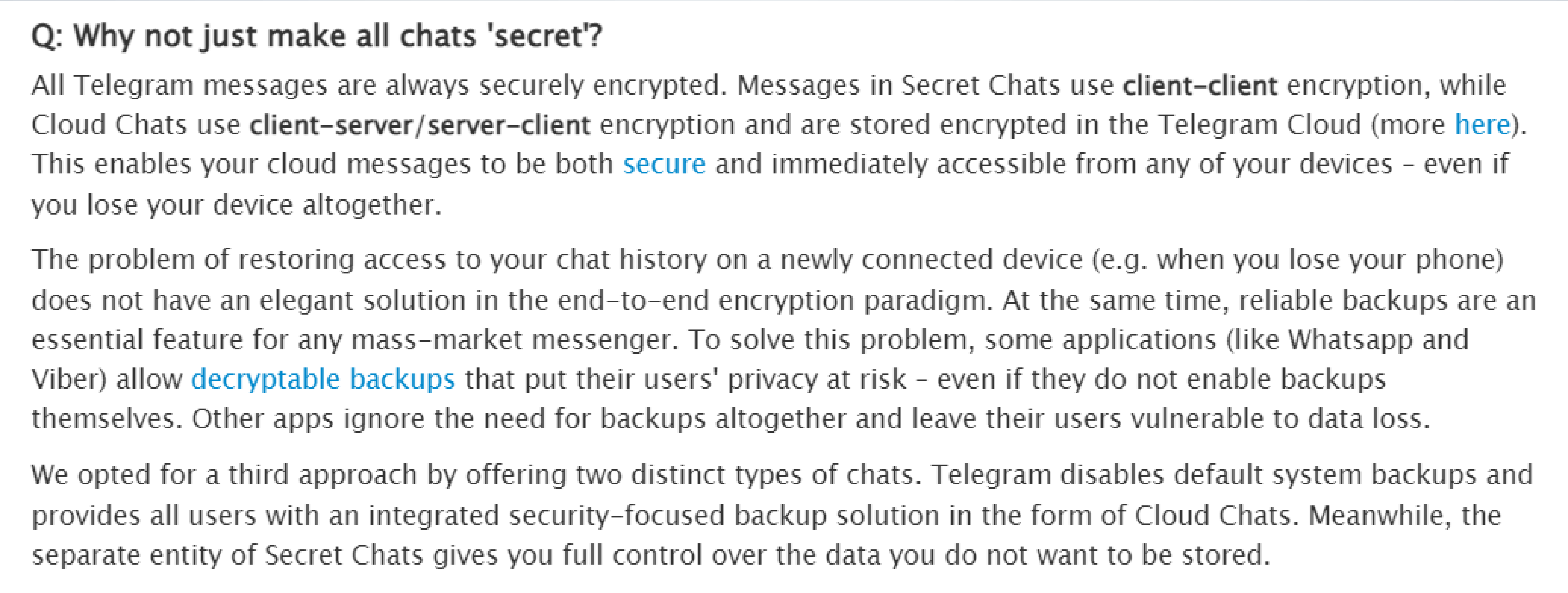
While other ways of achieving the same cryptographic goals undoubtedly exist, we feel that the present solution is both robust and also succeeds at our secondary task of beating unencrypted messengers in terms of delivery time and stability.

Q: Why are you mostly relying on classical crypto algorithms?

We prefer to use well-known algorithms, created in the days when bandwidth and processing power were both a much rarer commodity. This has valuable side effects for modern-day mobile development and sending large files, provided one takes care of the known drawbacks.

The weaknesses of such algorithms are also well-known, and have been exploited for decades. We use these algorithms in such a combination that, to the best of our knowledge, prevents any known attacks.

Telegram



Q: Why not just make all chats 'secret'?

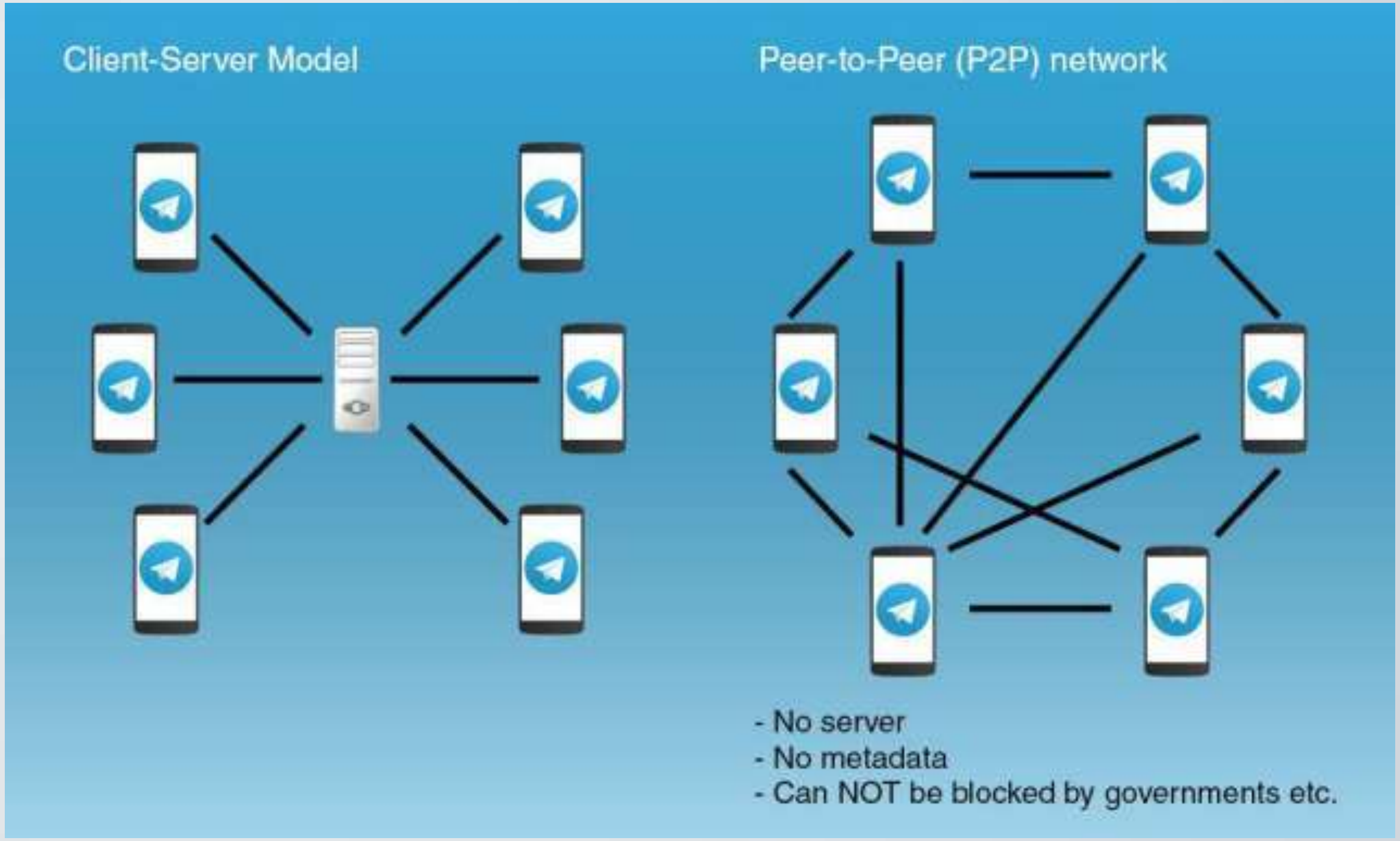
All Telegram messages are always securely encrypted. Messages in Secret Chats use **client-client** encryption, while Cloud Chats use **client-server/server-client** encryption and are stored encrypted in the Telegram Cloud (more here). This enables your cloud messages to be both secure and immediately accessible from any of your devices – even if you lose your device altogether.

The problem of restoring access to your chat history on a newly connected device (e.g. when you lose your phone) does not have an elegant solution in the end-to-end encryption paradigm. At the same time, reliable backups are an essential feature for any mass-market messenger. To solve this problem, some applications (like Whatsapp and Viber) allow decryptable backups that put their users' privacy at risk – even if they do not enable backups themselves. Other apps ignore the need for backups altogether and leave their users vulnerable to data loss.

We opted for a third approach by offering two distinct types of chats. Telegram disables default system backups and provides all users with an integrated security-focused backup solution in the form of Cloud Chats. Meanwhile, the separate entity of Secret Chats gives you full control over the data you do not want to be stored.

Telegram

Nel 2016, Telegram aveva iniziato a lavorare per implementare un tipo di crittografia peer-to-peer (P2P).

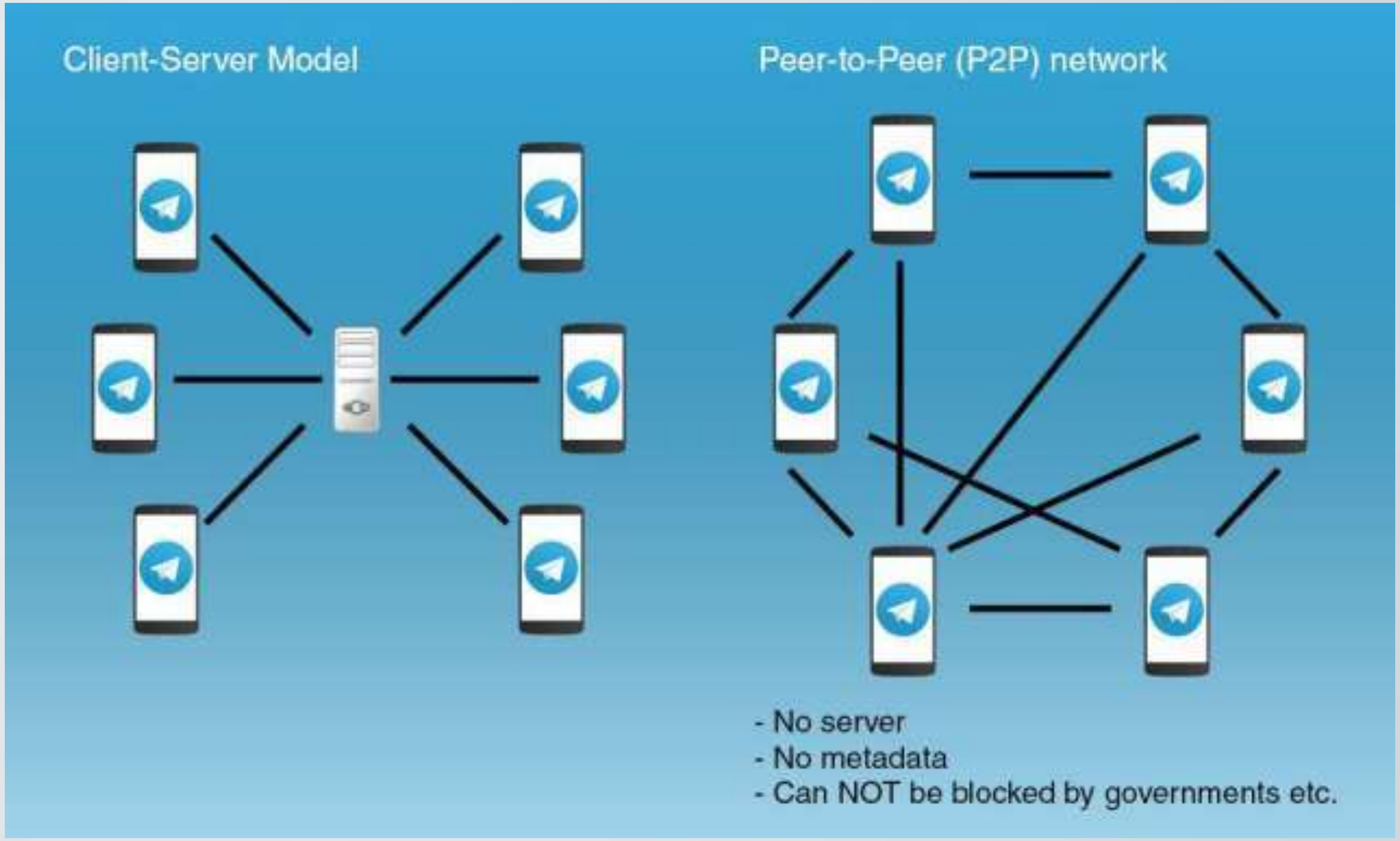


- No server
- No metadata
- Can NOT be blocked by governments etc.

Telegram

La crittografia P2P permetteva di staccarsi dalla dipendenza da un server.

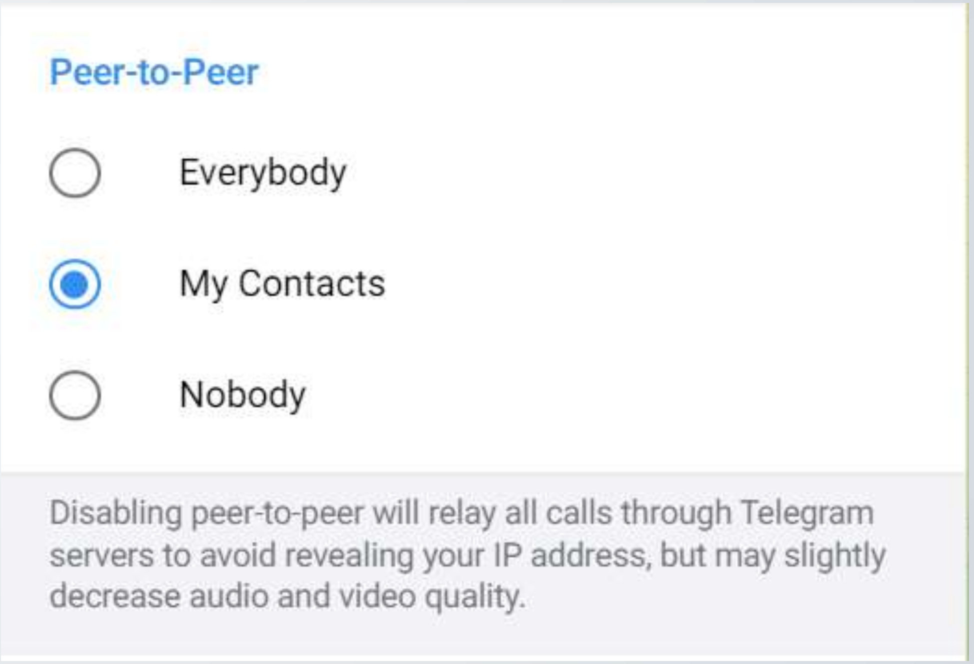
Il messaggio si crea e si distrugge continuamente passando per un circuito infinito di dispositivi connessi tra di loro.



- No server
- No metadata
- Can NOT be blocked by governments etc.

Telegram

Ad oggi, la crittografia peer-to-peer viene utilizzata da Telegram solo per le chiamate.



Peer-to-Peer

○ Everybody

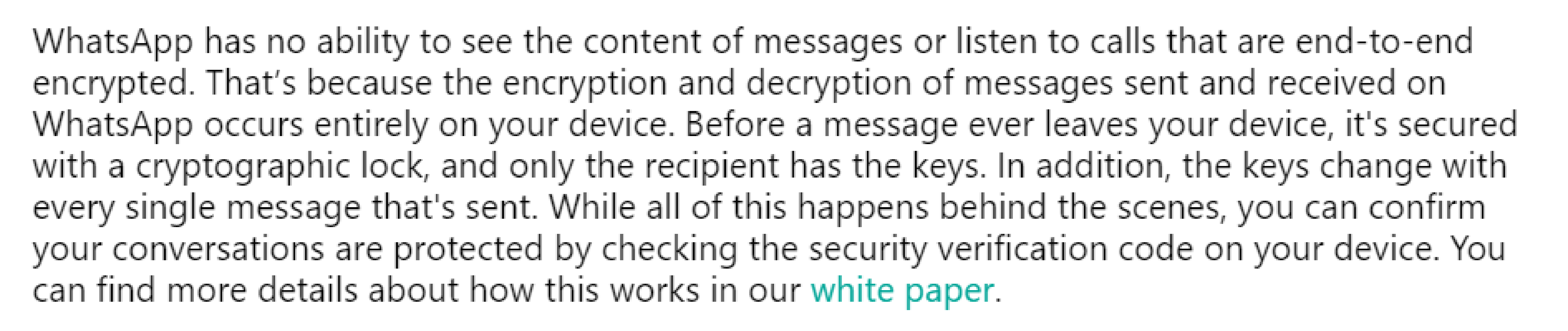
● My Contacts

○ Nobody

Disabling peer-to-peer will relay all calls through Telegram servers to avoid revealing your IP address, but may slightly decrease audio and video quality.

Whatsapp

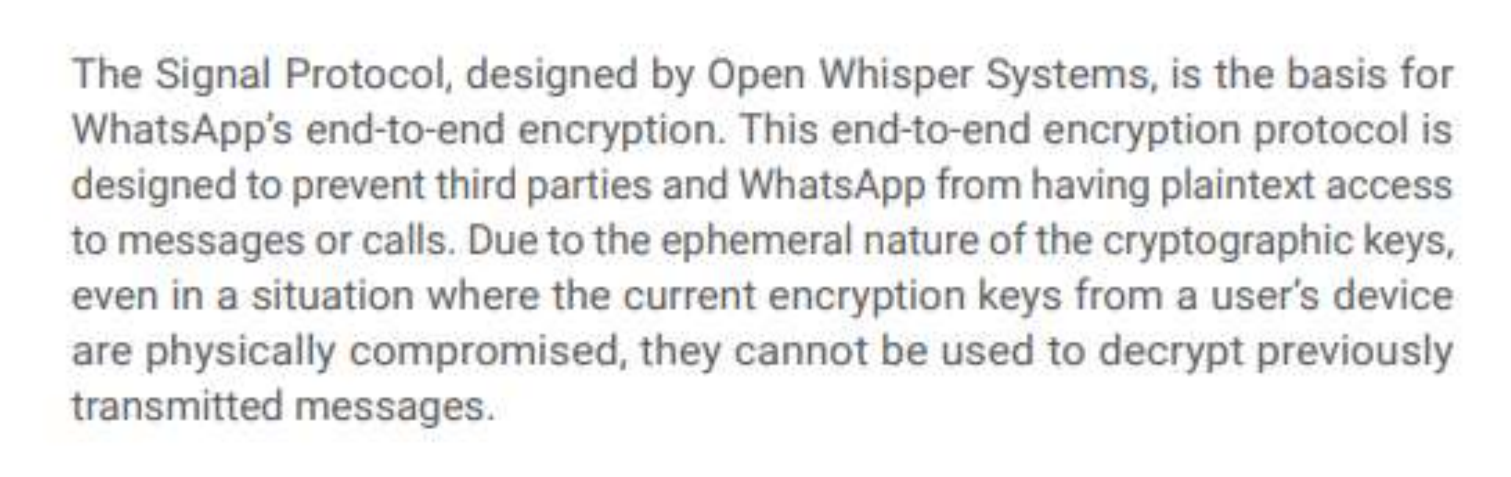
5 Aprile 2016: Whatsapp implementa la crittografia end-to-end



WhatsApp has no ability to see the content of messages or listen to calls that are end-to-end encrypted. That’s because the encryption and decryption of messages sent and received on WhatsApp occurs entirely on your device. Before a message ever leaves your device, it's secured with a cryptographic lock, and only the recipient has the keys. In addition, the keys change with every single message that's sent. While all of this happens behind the scenes, you can confirm your conversations are protected by checking the security verification code on your device. You can find more details about how this works in our white paper.

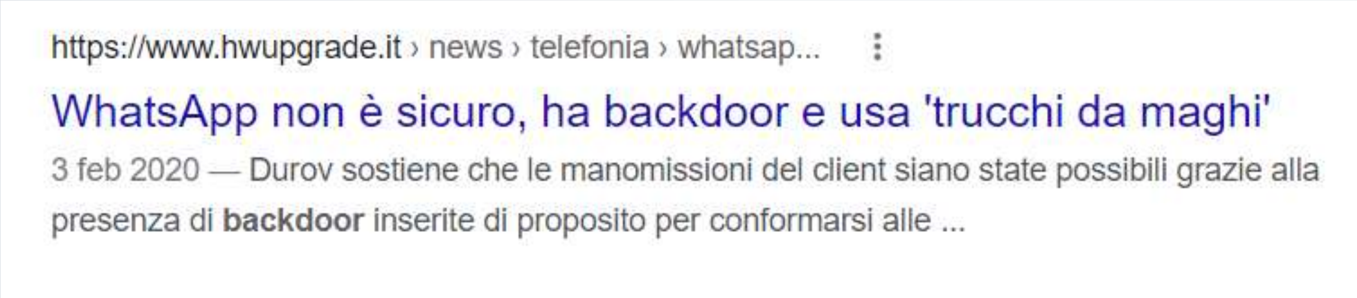
Whatsapp

Anche il Signal Protocol si basa su Diffie-Hellman e su AES



The Signal Protocol, designed by Open Whisper Systems, is the basis for WhatsApp's end-to-end encryption. This end-to-end encryption protocol is designed to prevent third parties and WhatsApp from having plaintext access to messages or calls. Due to the ephemeral nature of the cryptographic keys, even in a situation where the current encryption keys from a user's device are physically compromised, they cannot be used to decrypt previously transmitted messages.

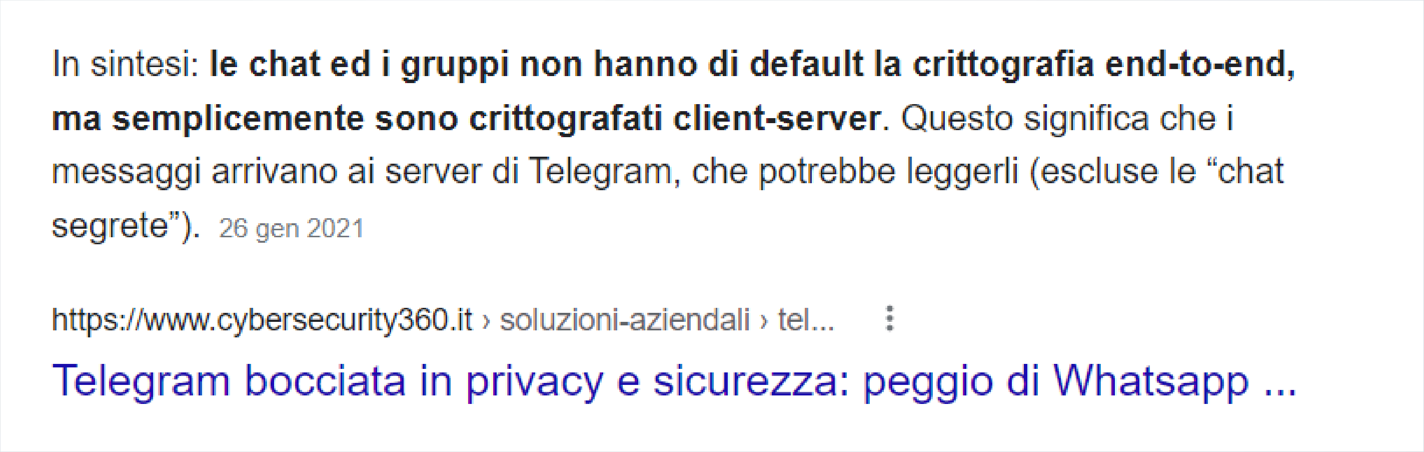
E quindi? Quale scegliamo?



https://www.hwupgrade.it › news › telefonia › whatsap...

WhatsApp non è sicuro, ha backdoor e usa 'trucchi da maghi'

3 feb 2020 — Durov sostiene che le manomissioni del client siano state possibili grazie alla presenza di **backdoor** inserite di proposito per conformarsi alle ...



In sintesi: **le chat ed i gruppi non hanno di default la crittografia end-to-end, ma semplicemente sono crittografati client-server**. Questo significa che i messaggi arrivano ai server di Telegram, che potrebbe leggerli (escluse le “chat segrete”). 26 gen 2021

https://www.cybersecurity360.it › soluzioni-aziendali › tel...

Telegram bocciata in privacy e sicurezza: peggio di Whatsapp ...

Link utili

- About end-to-end encryption – FAQ di Whatsapp - https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

- FAQ Telegram - https://telegram.org/faq#security