LINUX VAR

La S in HTTPS

Criptiamo il Web!

linuxvar.it · info@linuxvar.it

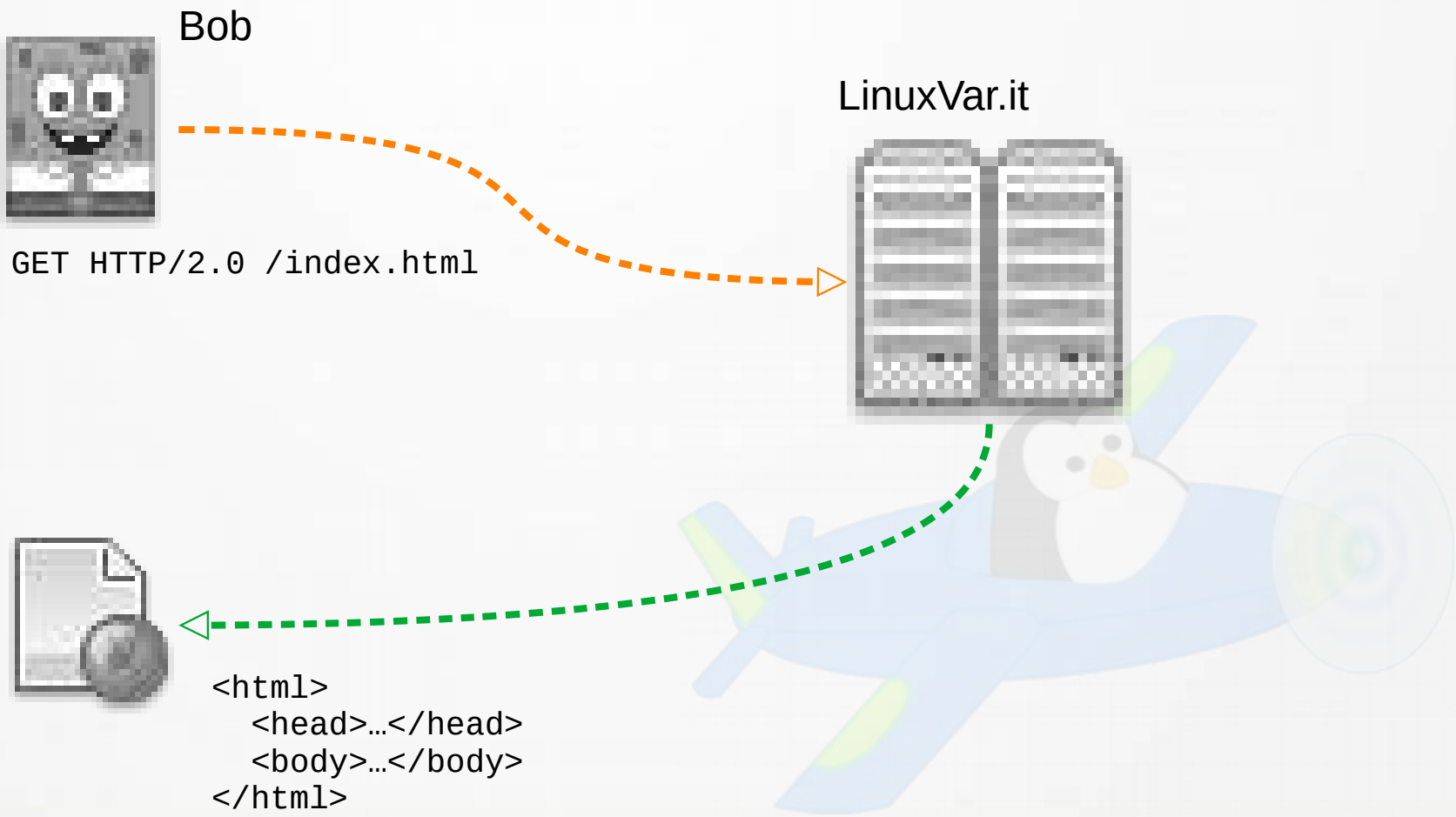
Chi sono

Ah, e questa foto contiene solo due colori, bianco e nero

- 26 anni
- “Neolaureato”
- Consulente “generalista”
- Sostenitore FOSS 
- Paranoico il giusto
- RicMa.co [https://ricma.co]

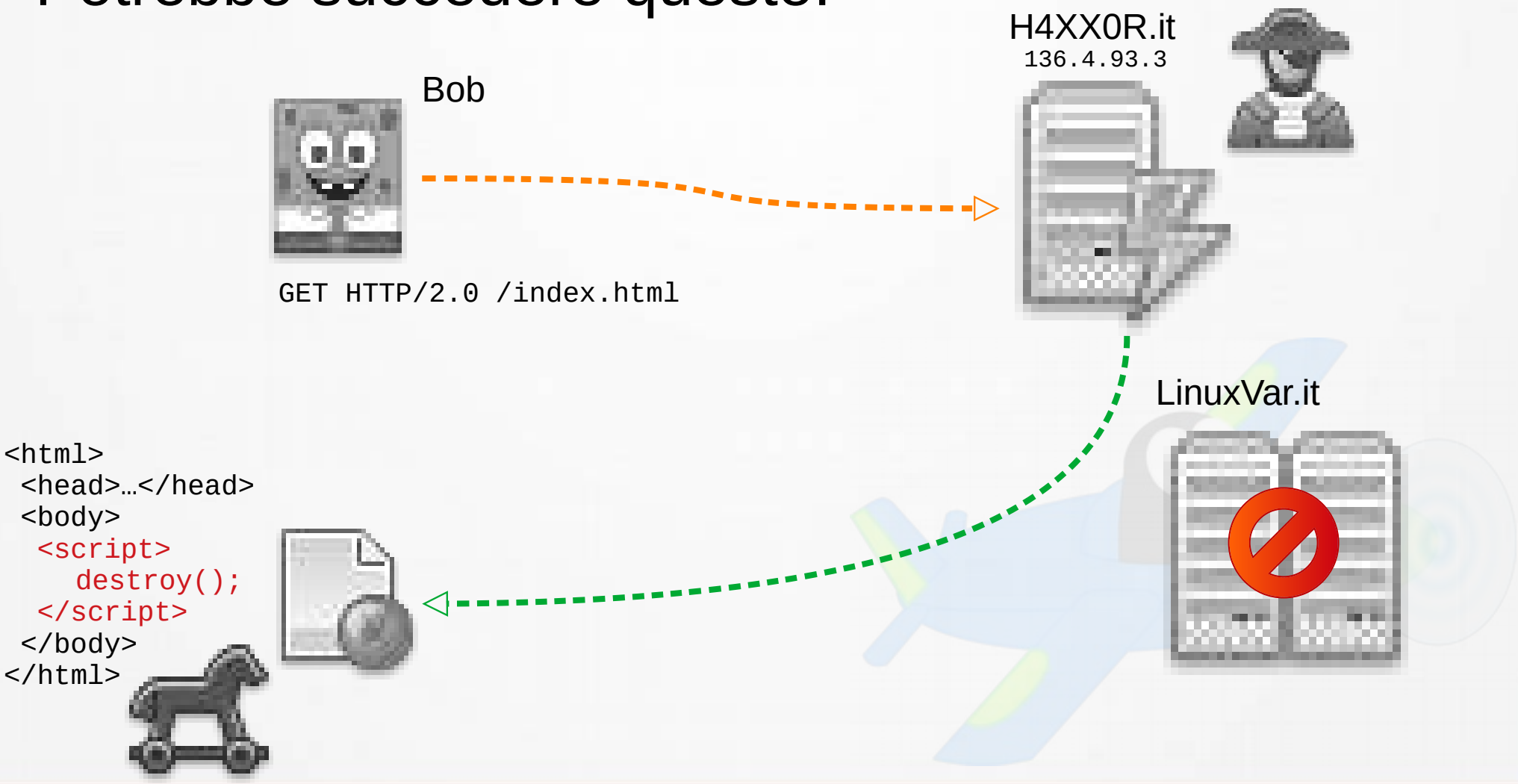
HTTP in breve

Si basa su **richiesta** e **risposta**:



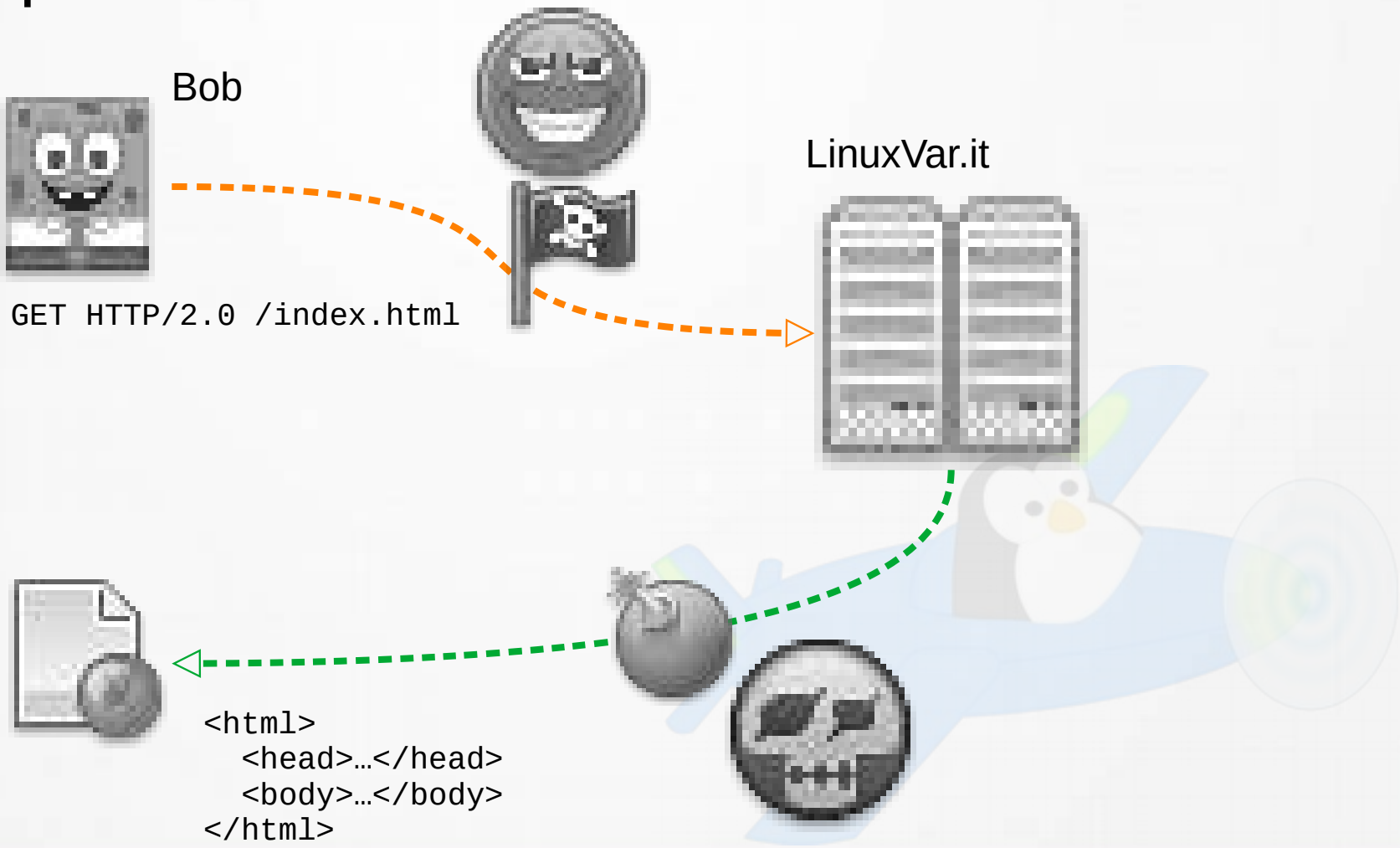
Problemi (1)

Potrebbe succedere questo:



Problemi (2)

Oppure questo:

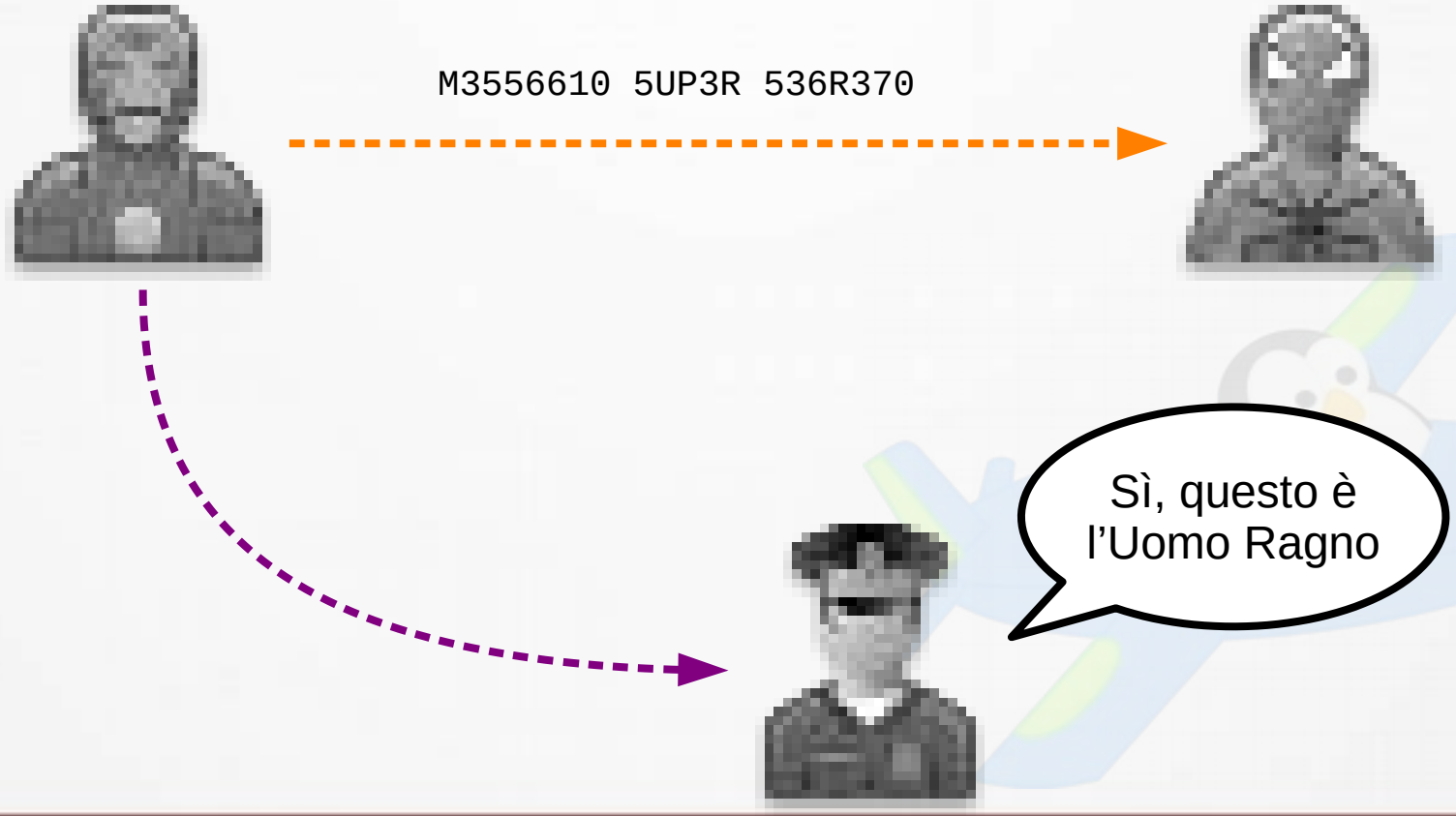


World *Wild* Web

- **Confidenzialità**: durante una comunicazione, è la protezione dei dati e delle informazioni tra un mittente e un destinatario nei confronti di terze parti
- **Integrità dei dati**: protezione dei dati e delle informazioni verso modifiche o rigenerazione del loro contenuto
- **Autenticazione**: confermare la verità di un dato o un'informazione, sostenuto vero da un'entità (da non confondere con *identificazione* o *autorizzazione*)

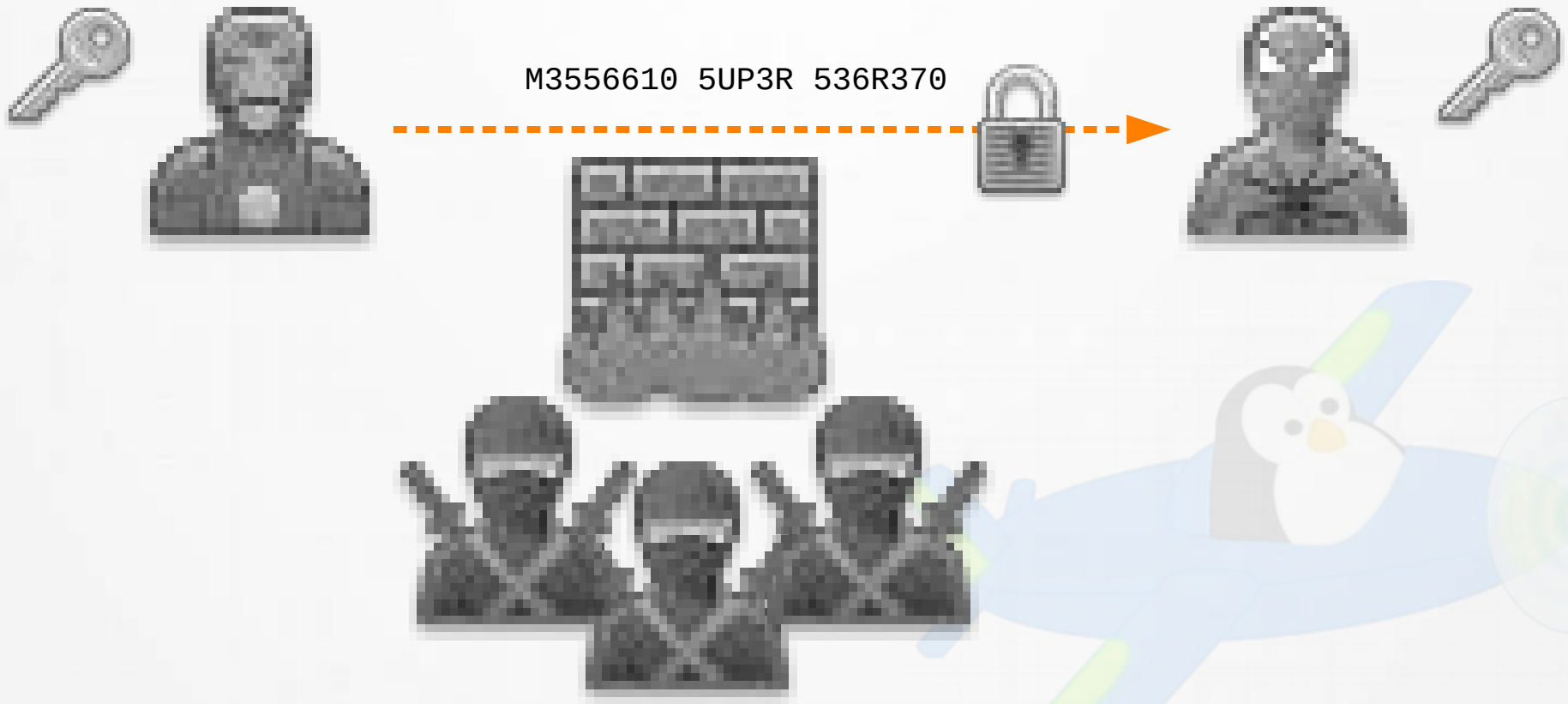
Garanzie di servizio (1)

- Sapere di star parlando *proprio* con chi vogliamo



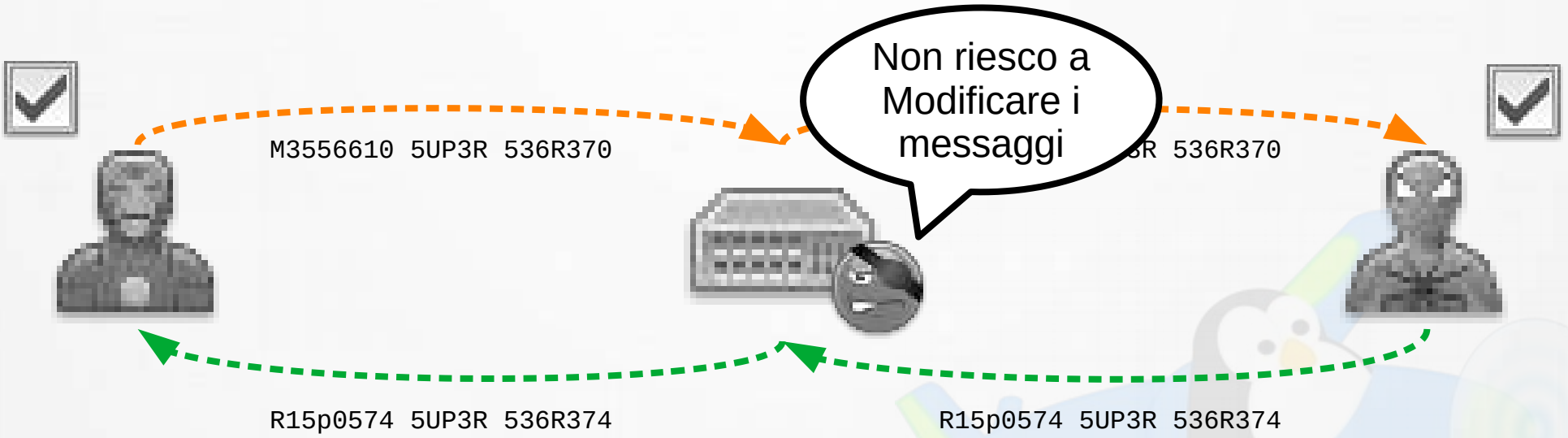
Garanzie di servizio (2)

- Avere un canale riservato e inaccessibile *a terzi*



Garanzie di servizio (3)

- Avere la certezza che nessuno possa *manomettere* i messaggi nel canale

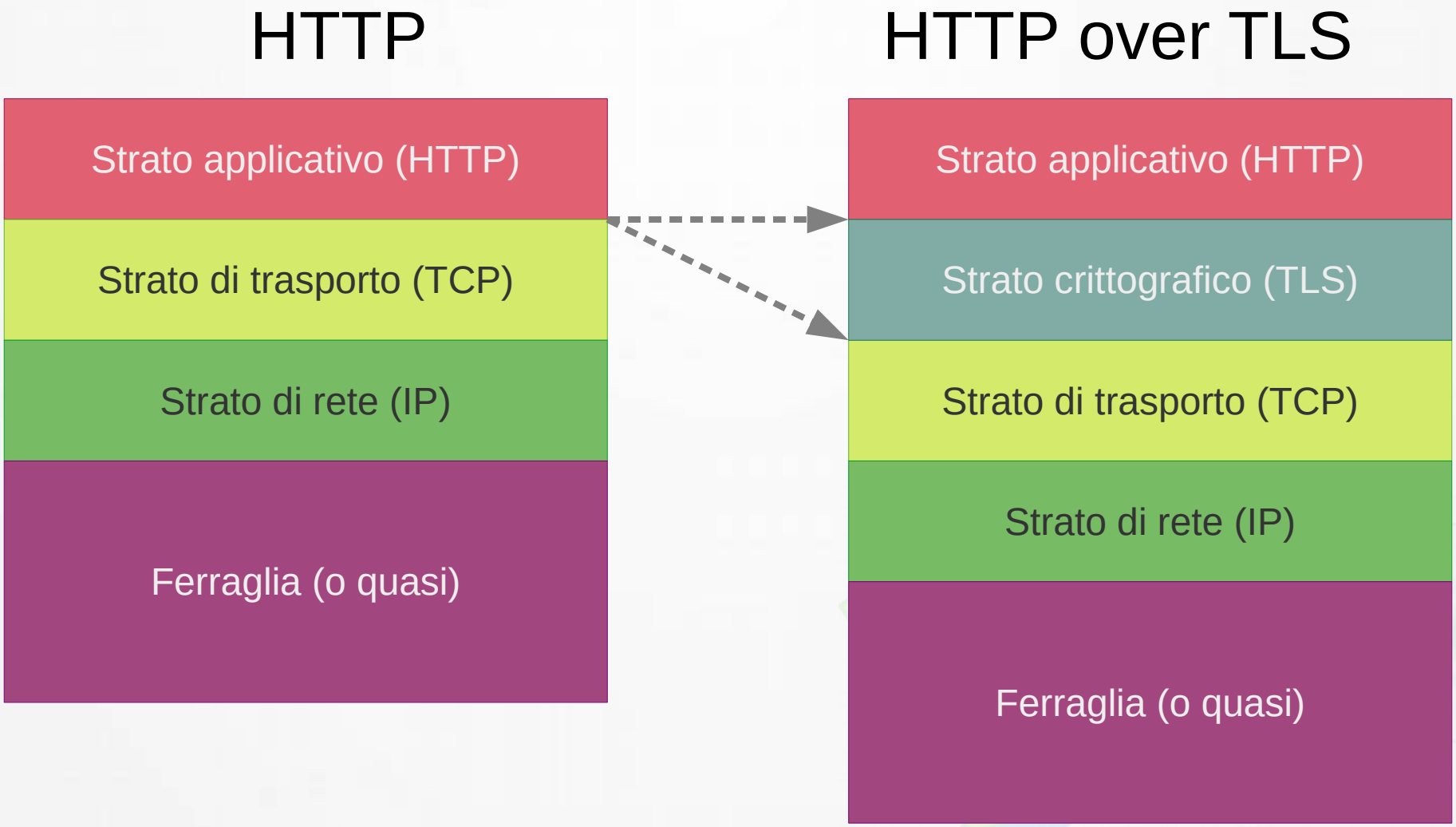


HTTPS… Si mangia?

- Più correttamente detto HTTP over **TLS** (o, in maniera *vintage*, HTTP over **SSL**)
- TLS (e, purtroppo, SSL) è «*un protocollo crittografico di presentazione* [che fornisce] *autenticazione*, *integrità dei dati* e *confidenzialità* *operando al di sopra del livello di trasporto*»*

* Transport Layer Security, http//it.wikipedia.org/w/index.php?title=Transport_Layer_Security&oldid=98482027 (in data 6 ottobre 2018).

HTTP vs HTTPS

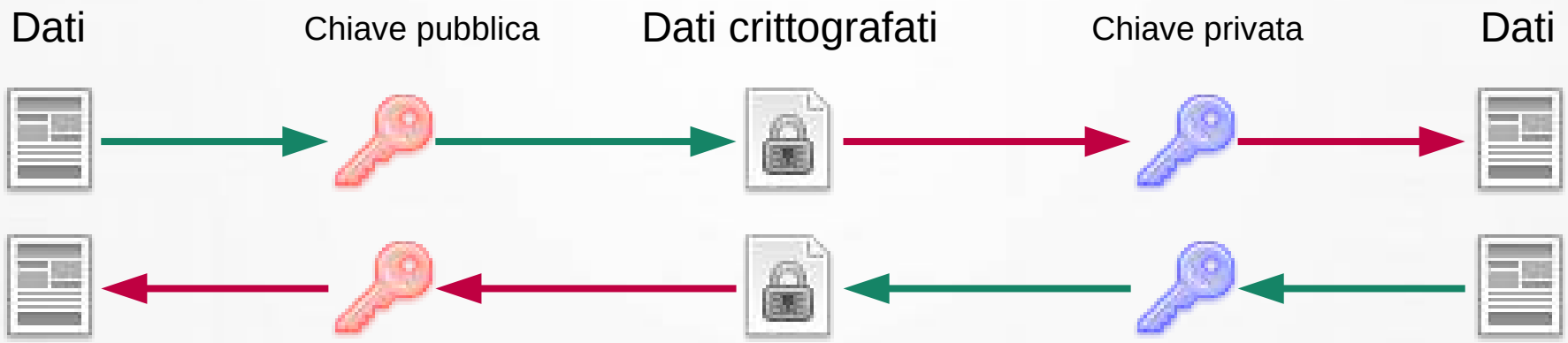


TLS: Transport Layer Security

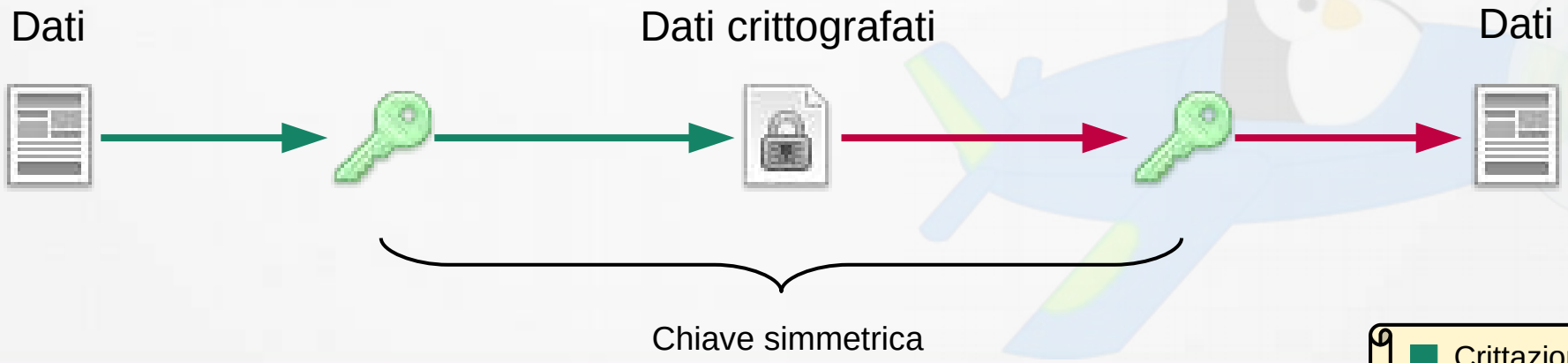
1. Utilizza una fase di *handshake* (stretta di mano) in cui
   a) i comunicanti concordano il tipo di strumenti utilizzati nella reale comunicazione
   b) il mittente verifica il passaporto del destinatario
   c) i comunicanti si scambiano un segreto comune
2. Viene stabilito un canale di comunicazione *stateful*, con le caratteristiche concordate
3. I due comunicanti iniziano l'interscambio dei dati sul canale

Inciso: cifratura a chiave

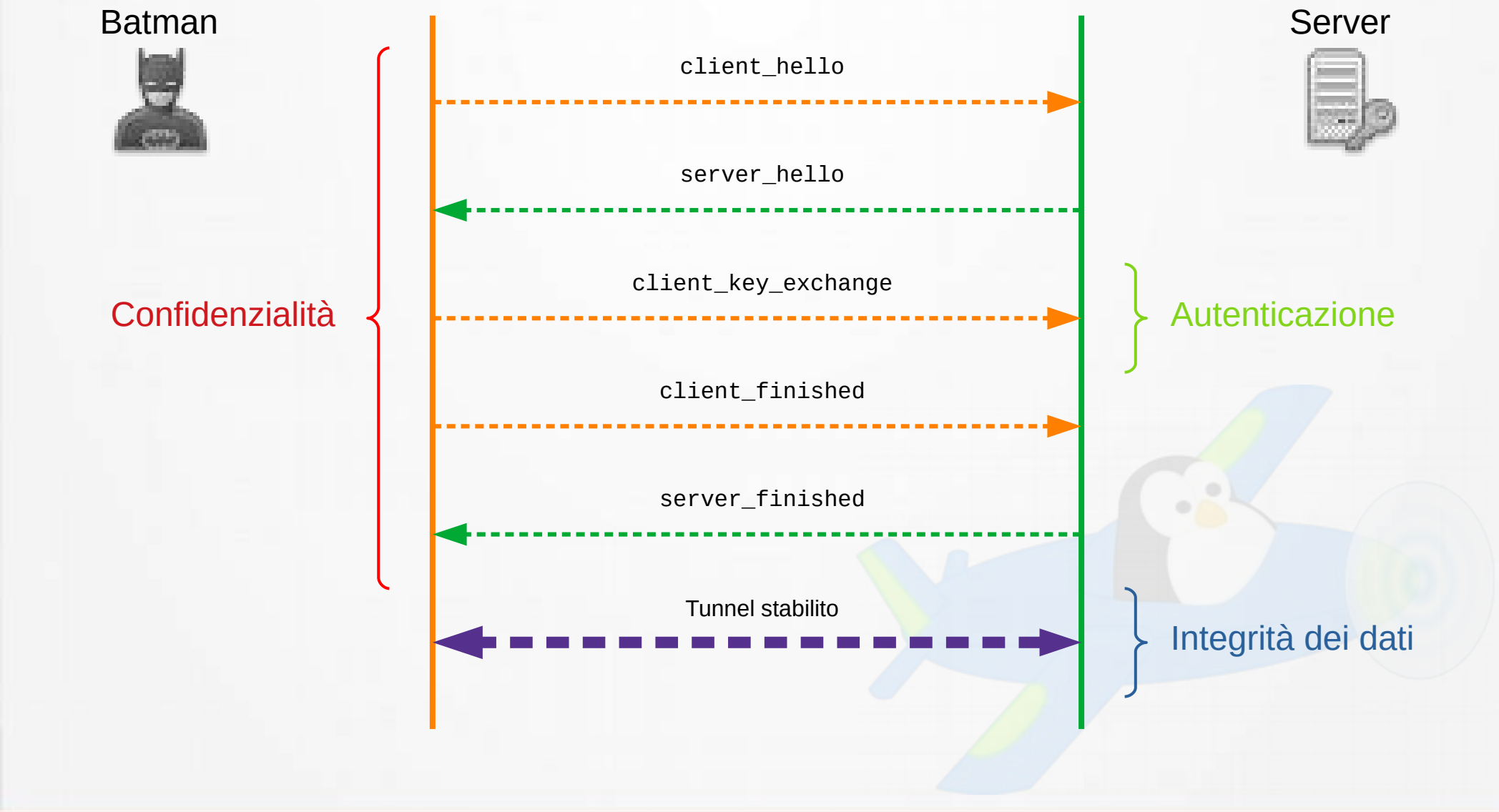
- Crittografia asimmetrica



- Crittografia simmetrica



Scambio di messaggi in TLS



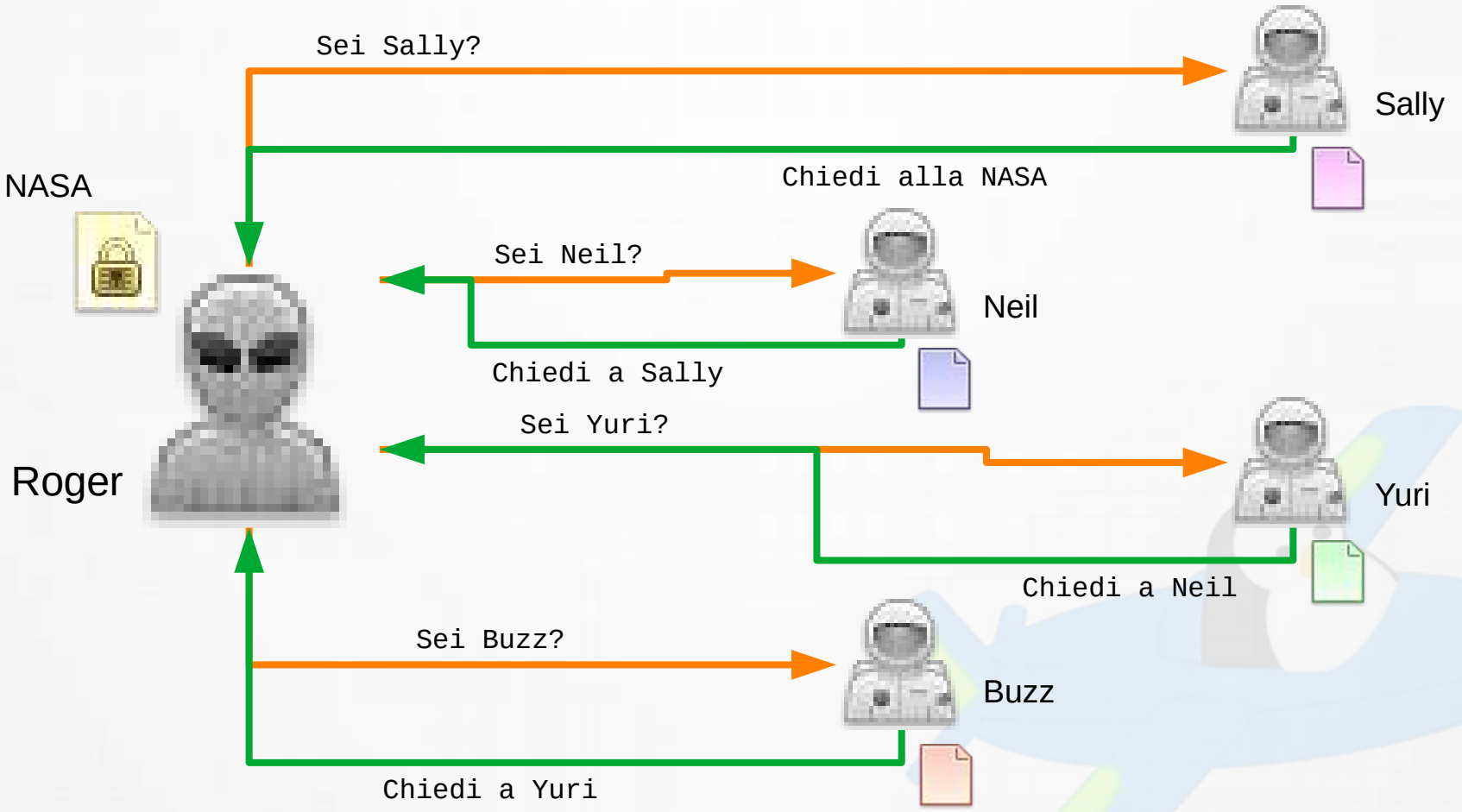
Messaggi (1)

- Client “`hello`”
  - Algoritmi di crittazione supportati
  - Numero random
  - Algoritmi di compressione supportati
- Server “`hello`”
  - Algoritmo di crittazione supportato
  - ID di sessione
  - Numero random
  - Certificato server
- Client “`key exchange`”
  - Numero random (crittato con la chiave server)
  - Certificato client (dopo aver controllato quello server)

Messaggi (2)

- Client “`finished`”
  - Messaggio crittato con la chiave condivisa
- Server “`finished`”
  - Messaggio crittato con la chiave condivisa
- Tunnel crittato stabilito
  - Ogni messaggio comprende un *hash* calcolato sul messaggio stesso e crittato con la chiave condivisa

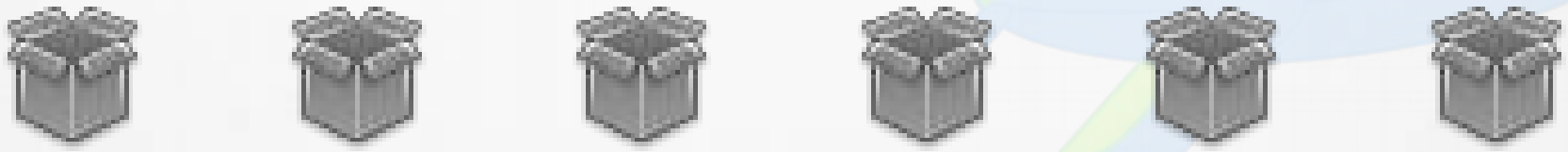
Certificati: *chain of trust*



Inciso: funzioni di *hash*

- Funzione matematica $h: N \rightarrow \{1,2,3,4,5,6\}$
  - Divide in parti uguali[1] l'insieme N
  - Es. `h = (n % 6) + 1`
  - Es. `h(42) = (42 % 6) + 1 = 1`

42



Grazie!

Riferimenti (1)

- **The First Few Milliseconds of an HTTPS Connection**, *http://www.moserware.com/2009/06/first-few-milliseconds-of-https.html* (in data 13 ottobre 2018)
- **How SSL-TLS Works**, *https://ldapwiki.com/wiki/How%20SSL-TLS%20Works* (in data 13 ottobre 2018)
- **Transport Layer Security**, *http//it.wikipedia.org/w/index.php?title=Transport_Layer_Security&oldid=98482027* (in data 6 ottobre 2018)
- **How does HTTPS actually work?**, *https://robertheaton.com/2014/03/27/how-does-https-actually-work/* (in data 6 ottobre 2018)
- **SSL/TLS Primer Part 1 - Data Encryption**, *https://blogs.akamai.com/2016/03/enterprise-security---ssltls-primer-part-1---data-encryption.html* (in data 6 ottobre 2018)

Riferimenti (2)

- **Secure Web Browsing - Computerphile**, *https://www.youtube.com/watch?v=E_wX40fQwEA* (in data 13 ottobre 2018)
- **Secret Key Exchange (Diffie-Hellman) - Computerphile**, *https://www.youtube.com/watch?v=NmM9HA2MQGI* (in data 13 ottobre 2018)
- **Transport Layer Security Protocol**, *https://docs.microsoft.com/en-us/windows/desktop/secauthn/transport-layer-security-protocol* (in data 13 ottobre 2018)
- **Asymmetric encryption - Simply explained**, https://www.youtube.com/watch?v=AQDCe585Lnc (in data 14 ottobre 2018)
- **An overview of the SSL or TLS handshake**, *https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm* (in data 23 ottobre 2018)