

Crittografia end-to-end

...

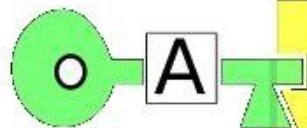
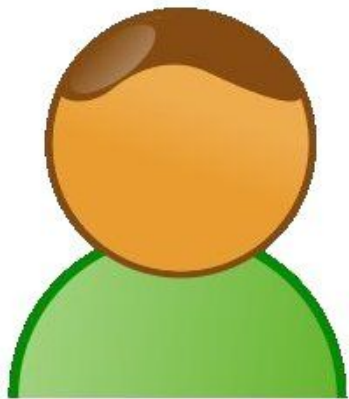
Riccardo Serafini

Linux Day 2017 - PDP FSUG Fabriano

Crittografia

(dall'unione di due parole greche: κρυπτός [kryptós] che significa "nascosto", e γραφία [graphía] che significa "scrittura")

è la branca della crittologia che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile/intelligibile a persone non autorizzate a leggerlo.

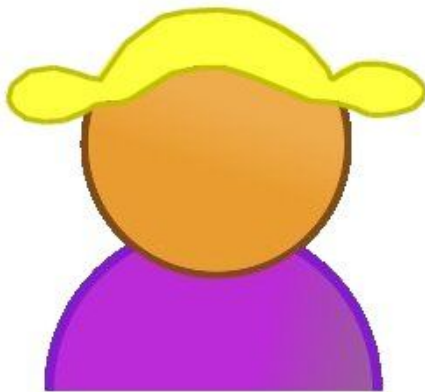


hello
Alice

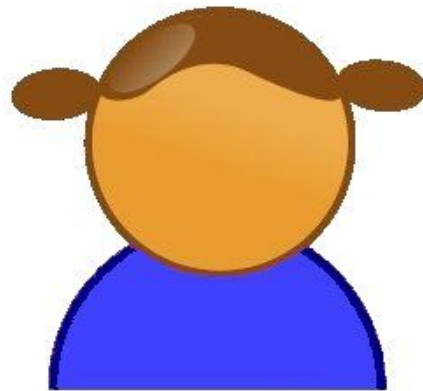


x0Ak3
o\$2Rj

Eve



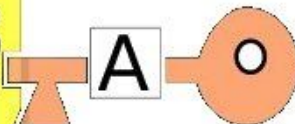
?



hello
Alice



x0Ak3
o\$2Rj



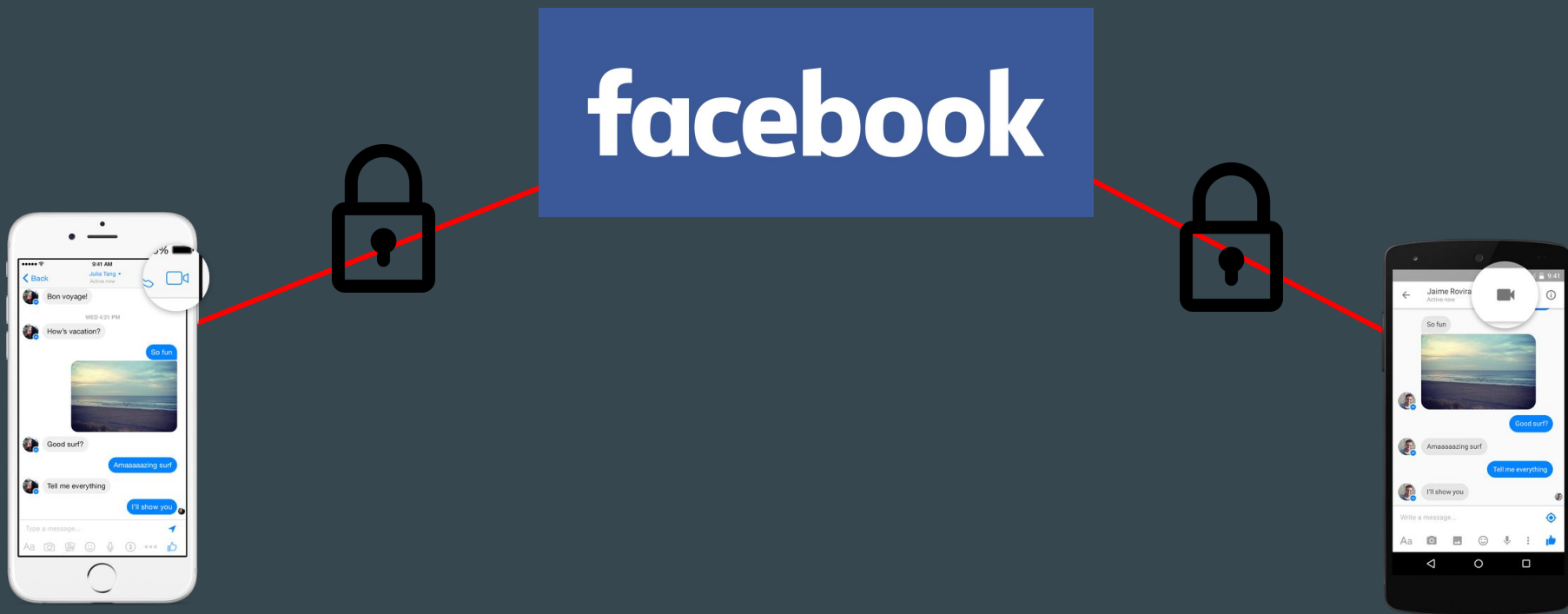
[illegible]

La utilizziamo tutti i giorni!



https://

Crittografia asimmetrica - modello client/server





Fabrizio Gaias

@fabriziogaias



Segui

Amici smanettoni, che vor di'? [#WhatsApp](#)

🔒 I messaggi che invii in questa chat e le chiamate sono ora protetti con la crittografia end-to-end.
Tocca per maggiori informazioni.



Scrivi un messaggio





 Daniel Ash

last seen 1 minute ago

*You have invited Daniel to join
a secret chat.*

Secret chats:

- Use end-to-end encryption
- Leave no trace on our servers
- Have a self-destruct timer
- Do not allow forwarding

Waiting for Daniel to get online...



Grazie

(per tutto il pesce)

Licenza slide: WTFPL