**Lez4 15/11/2024**

**meccaniche di whatsapp e telegram, messaggistica istantanea**

**Plain text**: A manda msg a B, msg passa in un server e poi arriva a B. msg è in chiaro(chiunque intercetta o qualsiasi cosa è leggibile e salvabile)

soluzione: cifratura, metodo Diffie-Helman e uso Crittografia AES (check passaggi in slide) (client-server)

messaggi non sono + in chiaro, ma i msgs sono gestiti dal o dai server e sempre alto rischio maninthemiddle

soluzione: crittografia end-to-end, server vede solo msg cifrato, senza decifrarlo, è ancora salvabile

aspetti Q&A di telegram che crea il

P2P (facilmente gestibile per enti governativi e polizia, e telegram se ne lava mani)

no server interlocutori, rete di dispositivi tra cui il msg raggiunge destinatario impacchettato in tante parti e passa tra tutti

es base di spotify

**La crittografia asimmetrica**

ci sono coppie di chiavi, una pubblica e una privata