PGP/GPG

un tempo c'era PGP = Pretty Good Privacy
ora c'è GPG = GNU Privacy Guard

25 febbraio 2014 – Circolo Pink Verona
Ilario Gelmetti e Collettivo Studiare con lentezza

Cos'è la cifratura/crittografia

Cos'è la cifratura/crittografia

- Io scrivo “Messaggio Segretissssimo”
- Cifro il messaggio in modo che si possa aprire solo con la chiave di Jonny, risulta “adffctetvc34xew3x2q4x43” e lo spedisco
- Il mio vicino di casa cracker vede il messaggio cifrato e non riesce a decifrarlo
- Il mio provider vede il messaggio cifrato e non riesce a decifrarlo
- La polizia italiana idem
- La polizia americana idem
- Il mio server di posta (esempio gmail) idem
- Il server di posta di Jonny (esempio Yahoo) idem
- Il provider di Jonny idem
- Il vicino di Jonny idem
- La mamma di Jonny idem

Cos'è la cifratura/crittografia

Solo Jonny riesce a decifrare il messaggio,
perché solo Jonny ha:

- il messaggio cifrato “adffctetvc34xew3x2q4x43”
- il file contenente la chiave segreta
- la password per sbloccare la chiave segreta

Cos'è la cifratura/crittografia

Tutti possono creare un messaggio per Jonny
Solo Jonny li può aprire

Cos'è la firma digitale

Al contrario funziona la firma digitale:
Solo Jonny può creare una firma a suo nome
Tutti possono verificare che sia corretta

Qual è la chiave di Jonny?

Ci sono dei siti con l'elenco delle chiavi esistenti. Se trovo più chiavi con nome Jonny come faccio a sapere qual è la sua chiave e quali sono false? (se usiamo la chiave creata da FintoJonny per cifrare un messaggio questo verrà letto da FintoJonny, anche la firma di FintoJonny ci sembrerà autentica)

Qual è la chiave di Jonny?

Ci sono più modi per capire qual è la chiave di Jonny:

- farsela dire di persona, non via mail (o farsi dire l'identificativo della chiave, più breve, ad esempio l'ID della mia chiave è 4CBBAA96)
- vedere se la forse chiave di Jonny è garantita da qualcuno di cui già ci fidiamo

Qual è la chiave di Jonny?

Vedere se la forse chiave di Jonny è garantita da qualcuno di cui già ci fidiamo.
Si chiama rete di fiducia, se alcuni miei amici di cui mi fido, mi garantiscono che quella chiave è davvero di Jonny allora mi fido anch'io.
Questo processo si può iterare, ma come le notizie indirette, più intermediari ci sono meno sono affidabili.
Dunque conviene sempre verificare di persona.

Ci sono rischi?

Per aprire un messaggio cifrato gli serve:
la tua chiave (un banale file sul tuo computer!)
e la tua password (non usare la stessa password
che usi sui servizi online/siti/forum)

Ci sono rischi?

Dunque se il pc lo tengo al sicuro e la password è diversa dalle altre che uso posso stare tranquillo?
Mica tanto.
Sistemi operativi chiusi (come Windows e MacOSX) contengono delle “entrate di servizio” riservate alle intelligence USA o delle falle create per sbaglio (?).

Meglio usare Linux

I sistemi operativi open source (Linux) possono essere verificati da soggetti indipendenti, possiamo (dobbiamo, non c'è di meglio...) fidarci che non siano state inserite backdoors che indeboliscano la nostra sicurezza.

Quali programmi usare?

Consiglio di usare il client email Thunderbird e di installarci l'estensione Enigmail.

Poi c'è da creare una chiave e da imparare ad usarla!