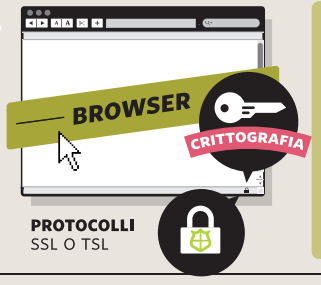
CIFRATURA CLASSICA (esempio: pagamento online)

01 IL COLLEGAMENTO

Un browser si collega a un sito per un'operazione (come pagamento online) che utilizza la crittografia come strumento di protezione

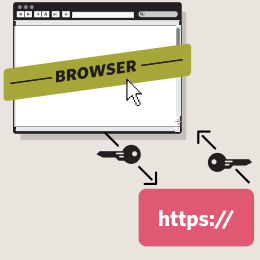


9 milioni
le persone vittima ogni anno di furto d'identità negli Stati Uniti

52,6
miliardi di dollari in danni arrecati dai furti

02 VERIFICA

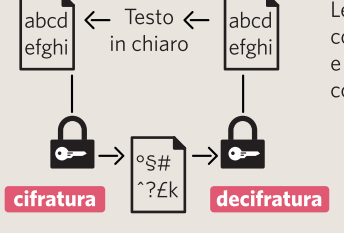
Il browser negozia (concorda) con il server del sito vari protocolli (algoritmi): di cifratura, di autenticazione (per accertare l'identità del sito) e di scambio di chiavi



La chiave è un insieme di bit che definisce come l'algoritmo deve cifrare i messaggi scambiati dalle due parti.

03 DIALOGO

Comincia la cifratura. È l'equivalente di tradurre i messaggi in un mucchio di lettere incomprensibili per chi non ha la chiave di decifratura.

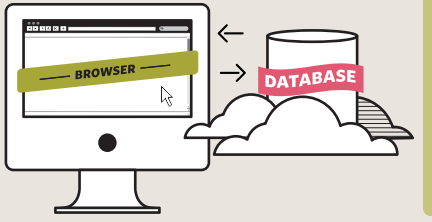


Le due parti continuamente cifrano e decifrano i messaggi con la stessa chiave

CIFRATURA OMOMORFICA (esempio: calcoli su dati medici)

01 CONNESSIONE

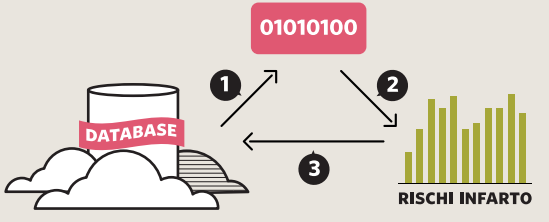
Un computer si collega a una piattaforma cloud computing con un database contenente informazioni cifrate su informazioni molto riservate (mediche, per esempio).



47%
di identità sono rubate da persone conosciute dalla vittima

02 RICHIESTA

Il computer chiede al servizio cloud di eseguire un calcolo sul database, per esempio un'analisi statistica dei rischi d'infarto o sulla ricorrenza di certi genomi



03 ELABORAZIONE

Il servizio esegue il calcolo senza decifrare le informazioni nel database. Fornisce la risposta, sempre cifrata, al computer dell'utente, che la decifra per conto proprio