CIFRARE QUALSIASI DOCUMENTO

Si vedono in rete forum e discussioni assurde.

Come posso cifrare un'intera cartella? (basta trasferirne il contenuto in un file ZIP!), e un file PDF? come faccio a cifrare un file DOC ecc..?

Falsi problemi. Infatti qualsiasi documento non è altro che una sequenza n di bytes, per cui l'unica cosa che conta è ottenere un file cifrato dove

byte (n) + algoritmo = byte cifrato (n)

e che si possa riottenere il documento originale con

byte cifrato (n) – algoritmo = byte (n)

Quale che fosse il tipo di documento, anche un testo in cinese, esso tornerà ad essere a disposizione delle applicazioni che lo utilizzano, con il suo contenuto e il suo nome originale.

CRITTOGRAFIA DOCUMENTI

Ai documenti cifrati puoi dare il nome che vuoi. Il nome del file di origine è memorizzato nel file cifrato per cui quando il documento viene decifrato gli viene assegnato in automatico il nome originale. Si puo scrivere un testo direttamente cifrato. Il sistema tiene aggiornato un archivio coi nomi die files cifrati e i corrispondenti documenti originali.

OPZIONE Zeta

Indica che stai cifrando un file cifrato. In questo caso ci sarà poi in automatico una doppia fase di decrittazione per ottenere il documento originale.

Questa opzione di cifratura estrema viene fornita non tanto per aumentare l'inviolabilità, ma più che altro a scopo dimostrativo delle possibilità del sistema. Di fatto si potrebbe continuare come in una sorta di matrioska di cifratura ottenendo un file cifrato con n chiavi.

AUTENTICAZIONE

Ogni documento cifrato contiene un codice identificativo (**NIDE**) irripetibile che esclude qualsiasi possibilità di manipolazione e certifica l'identità del mittente in modo sicuro.

Il sistema di cifratura è infatti tale che lo stesso documento, cifrato con la medesima chiave n volte, genera n files cifrati sempre diversi e quindi n **NIDE** diversi. (*v.sopra la nota tecnica)*

Il **NIDE** viene mostrato alla fine della cifratura, controllato dal sistema prima di decifrare ogni documento ed è comunque verificabile in qualsiasi momento con una funzione apposita e quindi mittente e destinatario possono assicurarsi della provenienza autentica del documento cifrato e della sua integrità.

Oltre al codice NIDE, vengono visualizzati:

- data di creazione

- nome della chiave utilizzata

- chi ha crittografato il documento

- nome del documento originale

IL FILE CHIAVI

Il file delle chiavi contiene tutte le chiavi dell'utente nella forma:

NOMEDELLACHIAVE (in chiaro, chiunque può vederlo) + CHIAVE (che solo tu puoi vedere, perchè cifrata con la **CHIAVE.DEL.FILE.DELLE.CHIAVI** che ti è stata chiesta all'inizio e che ti viene chiesta ogni volta che entri nel sistema).

Quindi una volta conosciuto il nome della chiave da utilizzare, viene estratta dall'archivio ed è solo il sistema che la può decifrare (con la **CHIAVE.DEL.FILE.DELLE.CHIAVI)** e permetterne l'utilizzo.
Il nome/riferimento relativo alla chiave viene memorizzato nei files cifrati e quindi la chiave per poi decifrare verrà prelevata senza dover dare alcuna indicazione.

Questa **CHIAVE.DEL.FILE.DELLE.CHIAVI** è l'unica che devi ricordare ma **DEVI** ricordarla altrimnti non potrai mai recuperare i files già cifrati perchè

può operare nel sistema solo chi conosce la CHIAVE.DEL.FILE.DELLE.CHIAVI

LE CHIAVI

Possono essere generate usando la funzione apposita del programma e poi assegnando loro il nome voluto.

Si può creare una chiave condivisa con un proprio corrispondente col procedimento di scambio delle chiavi disponibile nel sistema (op. 8)

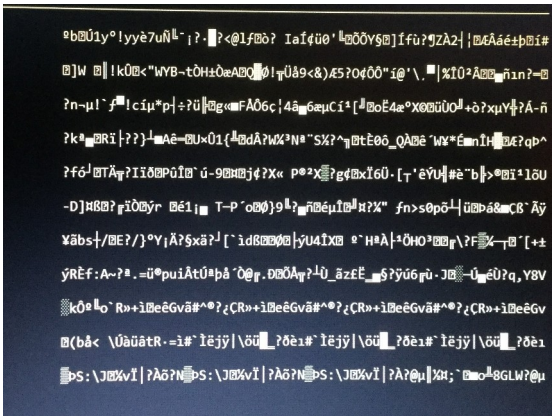
Il processo si svolge in 2 soli passaggi per creare una chiave condivisa K.

Il riferimento per K è il nome utente del corrispondente, che viene assegnato automaticamente e permette ad entrambi di decifrare correttamente i messaggi poichè su ogni file cifrato che verrà scambiato si troverà quel nome utente con cui la chiave condivisa è stata inserita nel file delle chiavi.

Alle chiavi create si può associare una descrizione per facilitare l'individuazione di un corrispondente.

Una chiave può anche essere importata nel sistema tramite un file che abbia nome **KIMPEXP e** che abbia il seguente formato **:** nome della chiave(24)+nome utente(24)+chiave(64)

La funzione che genera le chiavi permette di esportare la chiave generata sul file **KIMPEXP.** Si può fare una lista in cui si possono vedere tutte le chiavi (alcuni caratteri speciali non visualizzabili sono sostituiti da un ?). *a lato es. di chiavi*



IMPORTANTE: Non inserire mai una nuova chiave che abbia un nome uguale al proprio nickname.

Per un corretto layout :

- creare sul desktop un collegamento a Qcrypto

- clic tasto destro su icona del collegamento

- proprietà / layout

- in dimensioni finestra impostare 30 in altezza e 102 in larghezza

CAMOUFLAGE E UTILITIES

Con la funzione di camouflage puoi nascondere un documento A dentro un documento B.

B resta disponibile per qualsiasi applicazione, cioè se B fosse una foto la si vedrebbe esattamente come prima.

Con la funzione di decamouflage si estrae A.

per es. si potrebbe nascondere KIMPEXP dentro una foto da spedire al vs interlocutore e realizzare così uno scambio della chiave ragionevolmente sicuro. L'interlocutore farà il decamouflage e importerà la chiave dal **KIMPEXP** estratto dalla foto.

Si può cambiare la lingua di QCRYPTO, si può cancellare fisicamente un documento e nel caso si volesse trasmettere un documento veramente grande e non si avessero altri strumenti (pensiamo a un film di molti Giga) allora lo si può frazionare in tanti spezzoni della grandezza voluta potendo poi da essi ricostruire il documento originale.