Kalypso

Encrypting messages web service

Roberto Falconi (Ref.), Salvatore Licitra

Progetto per il Laboratorio di Architetture Software e Sicurezza Informatica

Kalypso è una web app di crittografia che si fonda sul principio di Kerckhoffs, il quale afferma che la sicurezza di un crittosistema non deve dipendere dall'occultazione dell'algoritmo, bensì dal tener segreta la chiave.

Criptazione

L'applicazione prevede la possibilità di inserire un qualsiasi messaggio testuale all'interno di una casella di testo, generare una chiave di crittografia e, infine, criptare il messaggio inserito visualizzando a schermo il risultato dell'operazione.

Un utente registrato potrà scrivere la propria chiave, di cui verrà indicato il livello di affidabilità, per consentirne una memorizzazione e una divulgazione più user-friendly; inoltre, a differenza di un utente non registrato, potrà criptare messaggi di qualsiasi lunghezza.

A questo punto sarà possibile copiare il messaggio crittografato ed inviarlo a chi si desideri, sapendo che esso sarà privo di alcun significato per chiunque altro; l'utente potrà decidere di salvare tale messaggio in un text file, in modo da poterlo trasferire e trasportare in completa libertà.

Al momento dell'encrypting verrà generato automaticamente un QR code, che si potrà salvare in un graphic file format e che sarà scannerizzabile tramite un qualsiasi QR code reader, in modo da trasferire il messaggio criptato senza lasciarne traccia sul computer.

Per una maggiore difesa dei messaggi inseriti, sarà anche possibile decidere per quanto tempo saranno essi decifrabili: si potrà scegliere infatti se permettere la decriptazione dei messaggi per un tempo indefinito, oppure se inserire un time-out a questi in modo che, qualora venga trafugata la chiave in un tempo superiore a quello impostato, il contenuto del messaggio sarà ormai impossibile da decifrare.

Lato server, per garantire trasparenza e affidabilità da parte degli amministratori, non verranno in alcun modo tracciati o registrati né i messaggi inseriti né le chiavi utilizzate dagli utenti.

Decriptazione

Una volta ricevuto un messaggio criptato tramite Kalypso, si dovrà tornare sull'applicazione web ed inserire testo e chiave di crittografia.

La chiave, dunque, dovrà essere comunicata al destinatario unitamente al messaggio: sarà premura degli utenti mantenere il segreto sulla chiave di crittografia per non consentire a terzi di decifrare i messaggi; una chiave conosciuta solo da un ristretto gruppo di persone potrà consentire di scambiare messaggi inaccessibili ad esterni.

Il messaggio potrà anche essere caricato direttamente a partire da un file di testo o dall'immagine del QR code.
Una volta inserito il messaggio criptato, una chiave, ed inviata la conferma, sarà possibile visualizzare il risultato della decriptazione e quindi il messaggio originale solo nel caso in cui la chiave immessa corrisponda davvero a quella corretta.

Autenticazione

I visitatori (utenti non registrati) potranno utilizzare pienamente le funzioni di criptazione e di decriptazione dei messaggi senza doversi registrare obbligatoriamente, tuttavia, ci si potrà iscrivere tramite il tradizionale metodo per username ed e-mail, utilizzati rispettivamente per il login e per l'eventuale ripristino della password. Da questo momento, oltre ai già citati privilegi, avranno a disposizione un menù per le impostazioni, dove potranno modificare username, e-mail e password.

Integrazione con il servizio REST

La generazione del QR code e la sua decriptazione saranno possibili grazie all'utilizzo delle API messe a disposizione da goqr.me. Questa parte è di fondamentale importanza poiché, per motivi di privacy, non esistono API da parte delle principali aziende tecnologiche che consentano l'inoltro (a partire da app di terzi come la nostra) di messaggi verso la nostra rete di amici. Infatti, sfruttando il QR code, riusciamo a passare il messaggio criptato su qualsiasi dispositivo dotato di scanner, rendendolo pronto all'inoltro su Social Network e servizi di Instant Messaging (quali Facebook, WhatsApp, Telegram, LinkedIn, i classici SMS ed e-mail, etc.) grazie alle opzioni di condivisione che garantiscono i sistemi operativi mobili a dispetto degli OS desktop.

Privilegi degli amministratori

L'amministratore del sito potrà inviare newsletter e avrà piena libertà di gestire il website ed i suoi utenti, potendoli cancellare e bannare.
Infine, gli sviluppatori potranno essere contattati dagli utenti per ricevere commenti, feedback o fornire assistenza.