PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5767 di Mercoledì 15 gennaio 2025

Cybersicurezza: Linee guida funzioni criptografiche

Un prezioso documento pubblicato dall'agenzia per la cybersicurezza nazionale (ACN) fornisce le indicazioni per orientarsi tra gli algoritmi crittografici, che permettono di proteggere le comunicazioni nel mondo digitale in maniera sicura ed efficiente.

L'agenzia per la cybersicurezza nazionale ACN ha cominciato a pubblicare preziosi documenti, che permettono di tenere aggiornati gli esperti di sicurezza informatica su tecniche di attacco e tecniche di difesa. Presentiamo oggi le "Linee guida funzioni criptografiche", un manuale dedicato all'illustrazione delle funzioni criptografiche

Linee guida funzioni criptografiche ? introduzione alla criptografia ed alle linee guida

Il documento, pubblicato nel luglio 2024, contiene un'introduzione al tema della criptografia, aggiornata alla data della pubblicazione. Il documento si preoccupa di segnalare ai lettori che la rapida evoluzione delle tecniche di attacco e difesa può rendere opportuno un frequente aggiornamento di questo documento.

Il documento passa in rassegna, in termini facilmente comprensibili, i concetti base della criptografia, cominciando dalla criptografia alfabetica dei tempi degli antichi romani, sino alle moderne tecniche di protezione, applicabili a documenti digitalizzati.

Di particolare interesse il capitolo dedicato alle tecniche di attacco, che comportano uso di computer quantistici. Al proposito, i nostri lettori sono stati costantemente informati circa il fatto che i computer quantistici possono rappresentare, allo stesso tempo, sia uno strumento di difesa, sia uno strumento di attacco. Il computer quantistico è uno strumento di difesa, quando può essere utilizzato per mettere a punto algoritmi crittografici difficilmente violabili, mentre diventa uno strumento di attacco, quando le sue potentissime capacità di calcolo vengono utilizzate per tentare di violare un algoritmo criptografico.

È bene chiarire che il documento ha un valore divulgativo e non deve essere considerato come un manuale per gli esperti di criptografia. Ciò non toglie che il suo valore sia decisamente elevato, sul piano della diffusione dell'informazione, perché aiuta molti soggetti, che potrebbero non avere una competenza specifica, a rendersi conto della architettura ed utilità degli algoritmi criptografici, accrescendo la sensibilità all'uso, anche in applicazioni non legate ad elaborazioni critiche. Un semplice applicativo criptografico può essere usato anche sul proprio telefono cellulare, in modo che i dati ivi presenti non possano essere catturati, in caso di furto.

Pubblicità

Al proposito, è bene ricordare che i telefoni cellulari, che sono dotati di strumenti di controllo dell'accesso, ad esempio grazie al riconoscimento dell'impronta digitale del possessore dell'apparecchio, non cifrano i dati in essi memorizzati e quindi, se in qualche modo si riesce a superare il blocco posto dal riconoscimento dell'impronta digitale, i dati sono liberamente accessibili.

Se invece i dati sono successivamente protetti da un algoritmo criptografico, l'attaccante deve superare un nuovo ostacolo, spesso assai impegnativo, che comporta la individuazione della chiave di decodifica.

Ecco il motivo per cui l'agenzia per la cybersicurezza nazionale ha pubblicato anche un altro volume, destinato specificamente alle modalità di conservazione sicura delle password. Questo tema è oggetto di un'analisi nella seconda parte di questo articolo.

Agenzia per la Cybersicurezza Nazionale - Linee guida funzioni crittografiche - Introduzione alla Crittografia e alle Linee Guida

Adalberto Biasiotti

Licenza Creative Commons

www.puntosicuro.it