PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5805 di Lunedì 10 marzo 2025

Cybersicurezza: Linee guida Cifrari a Blocchi

Un responsabile della sicurezza informatica deve leggere attentamente le linee guida funzioni crittografiche pubblicate dall'agenzia per la cybersicurezza nazionale. Questo manuale prende in considerazione i cifrari a blocchi.

L'interesse manifestato dai nostri lettori sulla illustrazione dei manuali dell'agenzia per la cybersicurezza nazionale sulle funzioni crittografiche ci incoraggia nel continuare ad illustrare questi preziosi documenti.

In particolare, questo documento illustra una tecnologia di protezione crittografica, basata sui cifrari a blocchi. Questi sono i metodi di crittografia oggi più diffusi nell'ambito delle comunicazioni digitali.

Si tratta di sistemi simmetrici, che utilizzano in fase di cifratura e decifratura la stessa chiave, che evidentemente deve essere nota soltanto ai legittimi interlocutori e non deve essere accessibile a nessun altro.

La caratteristica di questi applicativi crittografici è definita dal nome stesso, in quanto essi operano su porzioni del testo in chiaro di lunghezza prefissata, chiamate appunto blocchi.

Un messaggio in chiaro viene suddiviso in blocchi e l'algoritmo provvede a cifrare ogni singolo blocco. Solo chi è in possesso della chiave può ricostruire il messaggio di partenza, tramite calcolo inverso. L'elevato livello di sicurezza di questi algoritmi discende dal fatto che la chiave segreta viene utilizzata per generare più chiavi intermedie. Col passare del tempo e con l'aumento di potenza di calcolo dei computer, le chiavi a 64 bit, inizialmente utilizzate, sono state successivamente allungate fino a 128 bit e, in qualche caso, perfino con lunghezze maggiori. Il secondo capitolo di questo manuale illustra le varie tecniche di cifrari a blocchi oggi disponibili, in grado di garantire la sicurezza delle comunicazioni.

L'intero terzo capitolo è dedicato alla illustrazione delle tecniche di attacco dei cifrari a blocchi. Una delle prime tecnologie di attacco, negli anni 90, sfruttava l'individuazione di possibili relazioni lineari tra i blocchi del testo in chiaro ed i blocchi del testo cifrato.

Al proposito, chi scrive coglie l'occasione per ricordare ai lettori una tecnica di violazione di un algoritmo criptografico, utilizzata durante la seconda guerra mondiale. Gli esperti di decrittazione esaminarono un certo numero di messaggi, che venivano scambiati tra le forze armate tedesche. Tutti questi messaggi erano dotati di un'intestazione, che veniva anch'essa cifrata. Mettendo a confronto i testi cifrati di vari messaggi, si poté scoprire, conoscendo già il significato in chiaro del primo blocco del testo cifrato, qual era la chiave di cifratura!

Un'altra tecnica di analisi è stata battezzata criptoanalisi differenziale e fu messa a punto nei primi anni 90 per attaccare uno dei più diffusi cifrari allora in uso, vale a dire il DES (digital Encryption standard). Non dimentichiamo infine che lo scenario di rischio è certamente aumentato negli ultimi tempi, grazie alla possibilità di utilizzare computer quantistici come strumenti di attacco.

Il quarto capitolo è dedicato alla illustrazione dell'algoritmo criptografico che nel 2001 vinse la competizione pubblica lanciata dal NIST: lo AES ? Advanced Encryption standard, che è oggi l'algoritmo più diffuso nell'ambito della cifratura a blocchi. La lunghezza dei blocchi coinvolti è di 128 bit.

Il quinto capitolo è dedicato alla illustrazione delle modalità di funzionamento dei cifrari a blocchi, illustrando pregi e difetti delle varie modalità disponibili. Particolare attenzione viene prestata alla rapidità di cifratura, che rappresenta un elemento vantaggioso nell'utilizzo quotidiano.

Il sesto capitolo è dedicato alla illustrazione delle tecniche di padding, vale a dire le tecniche che permettono di rendere tutti i blocchi della stessa lunghezza, indipendentemente dalla lunghezza presente nel messaggio originale. Ciò può comportare il fatto che la lunghezza del testo cifrato possa essere maggiore rispetto a quella del messaggio in chiaro e occorre che il destinatario del messaggio, che deve procedere alla decifrazione, conosca la tecnica utilizzata dal mittente per rendere tutti i blocchi della stessa lunghezza, aggiungendo bit ove necessari.

Il manuale si conclude, al capitolo 7, con la raccomandazione di utilizzare solo l'algoritmo AES, con appropriata lunghezza della chiave.

Buona lettura a tutti

Agenzia per la Cybersicurezza Nazionale - Linee guida funzioni crittografiche - Cifrari a Blocchi e Modalità di Funzionamento.

Adalberto Biasiotti

Leggi gli articoli con le altre linee guida:

Cybersicurezza: Linee guida funzioni criptografiche

Cybersicurezza: Linee guida conservazione delle password

www.puntosicuro.it