SLIDE1: INTRO

Nell'ambito della crittografia possiamo far rientrare anche le funzioni di hashing. Con questo termine si intendono delle funzioni crittografiche one-way che permettono di ricavare da un testo di lunghezza arbitraria una stringa di lunghezza predefinita, chiamata hash/digest/impronta. La particolarità di queste funzioni è che ogni stringa genera un digest diverso, anche se il testo originario varia di pochi bit. Altra particolarità è il fatto che, essendo funzioni one-way, il calcolo dell'hash richiede tempi brevissimi, mentre è praticamente impossibile il calcolo inverso.

SLIDE2: MD5

Un algoritmo di hashing ampiamente utilizzato è MD5, il quale produre un hash di 128 bit, solitamente rappresentato con 32 cifre esadecimali. Come si vede dall'esempio il cambiamento di un solo carattere nel testo originario provoca un cambiamento radicale nell'hash. Dato che MD5 presenta alcune falle, sostanzialmente collisioni (termine col quale si indicano due stringhe diverse che producono lo stesso hash) sono stati sviluppati nuovi algoritmi.

SLIDE3: SHA

Per colmare queste falle infatti la National Security Agency ha rilasciato l'algoritmo SHA. In seguito è stato modificato varie volte fino ad arrivare alla cosiddetta famiglia SHA, un insieme di algoritmi di hashing che comprende SHA-0, SHA-1 e SHA-224, SHA-256, SHA-384 e SHA-512. Ad eccezione di SHA-0 e SHA-1, il nome rappresenta la lunghezza dell'hash generato. SHA-0 è ritenuto insiscuro pertanto è consigliabile utilizzare SHA-1.

SLIDE4: MD5 REVERSE

Esistono degli strumenti online che permettono il calcolo dell'hash di una stringa. Talvolta permettono di ottenere il testo originario partendo dall'hash. Ciò è possibile grazie al fatto che durante il calcolo dell'hash vengono salvate le corrispondenze all'interno di un database e ciò che viene presentato all'utente come un calcolo dell'inverso in realtà è una ricerca all'interno del database degli hash già calcolati. Pertanto, dato che molte password vengono salvate in MD5, non si dovrebbero mai scegliere password comuni o di default, perché sicuramente le relative corrispondenze si trovano già all'interno di questi database.

SLIDE5: INTEGRITÀ

le funzioni di hashing permettono di verificare l'integrità di un messaggio, cioè che non sia stato alterato durante la trasmissione. Questo è possibile semplicemente generando l'hash del messaggio prima di inviarlo e una volta ricevuto. Se i due hash corrispondono il messaggio non è stato alterato.

SLIDE6: FIRMA DIGITALE

Dette funzioni di hashing permettono anche di firmare digitalmente un documento, garantendone la provenienza e quindi l'identità del mittente. Ciò avviene generando l'hash del messaggio, cifrandolo con la propria chiave privata e aggiungendolo in coda al messaggio da firmare. Il destinatario che vorrà controllare l'autenticità della firma dovrà semplicemente dividere il messaggio dall'hash, calcolarne l'impronta e verificarla con quella in calce messaggio. In questo modo integrità e provenienza del messaggio sono garantite.