

S-vLab

Integrità, funzione hash
e numeri pseudocasuali

Anna Riccioni
anna.riccioni@unibo.it

Sicurezza dell'Informazione M

Esercitazione del 23 marzo 2010

Tecniche di codifica dei dati

Encoding

- Codifiche disponibili:

- UTF-8
 - UTF-16
 - HEX
 - BASE-64
- stringhe, file di testo
- file binari, file in formati complessi

- HEX e BASE-64 consentono di rappresentare in formato testuale il contenuto di byte che le codifiche ASCII o UTF associano a caratteri non stampabili

BASE-64

- Codifica in BASE-64:

- anziché considerare un byte alla volta, se ne considerano 3

01010101	00000000	11111111
----------	----------	----------

- i 24 bit che compongono i 3 byte possono essere suddivisi in 4 blocchi da 6 bit l'uno

010101	010000	000011	111111
--------	--------	--------	--------

- un blocco di 6 bit ha 2^6 possibili configurazioni, ognuna delle quali è associata, nella codifica BASE-64, ad uno dei 64 caratteri stampabili nell'insieme [A..Z] U [a..z] U [0..9] U {+} U {/}

BASE-64

- una codifica in BASE-64 trasforma la sequenza di byte di partenza in una nuova sequenza di byte, leggibile in forma testuale, ma la cui dimensione risulta incrementata di un terzo
- poiché si considerano 3 byte per volta, nel caso in cui la sequenza di byte di partenza non abbia una lunghezza multipla di 3 occorre utilizzare un "padding":
 - un eventuale blocco in BASE-64 incompleto viene riempito di "0" fino a raggiungere la dimensione di 6 bit
 - eventuali blocchi da 6 bit mancanti vengono sostituiti dal carattere speciale "="

BASE-64: esempio

H e l l o

01001000	01100101	01101100	01101100	01101111
----------	----------	----------	----------	----------

010010	000110	010101	101100	011011	000110	111100	XXXXXX
--------	--------	--------	--------	--------	--------	--------	--------

S G V s b G 8 =



