Esercitazione Crittografia n°1

(5Bi - Lab di Tecnologie – 08/01/2018)

Utilizzando l'esempio di codice ed il materiale fornito viene richiesta la realizzazione di una applicazione C# (GUI) in grado di realizzare le seguenti funzioni di base:

Cifratura:

- Selezionare uno o più file (file "in chiaro" e tutti nella stessa cartella).
- Richiedere il nome nella directory di destinazione.
- Richiedere la chiave simmetrica di cifratura
- Cifrare il/i file scrivendoli poi nella directory di destinazione. I file dovranno avere estensione "*.ACM" (Algoritmo Crittografico Marconi) e per ogni file viene anche calcolato e scritto il corrispondente valore MD5 (si veda esempio allegato).
- Visualizzare il "Log" delle operazioni svolte.

Decifratura:

- Selezionare uno o più file (file cifrati ed in una stessa cartella, con estensione *.ACM).
- Richiedere il nome nella directory di destinazione.
- Decifrare il/i file scrivendo il/i file originale nella directory di destinazione.
- Visualizzare il "Log" delle operazioni svolte.

Verifica MD5:

- Selezionare uno o più file ACM (tutti nella stessa cartella).
- Verificare che il valore di MD5 ricalcolato coincida con quello memorizzato nel file.
- Visualizzare il "Log" delle operazioni svolte.

Viene richiesta anche la realizzazione di una **"Test Unit"** per il "Test", in automatico, della classe "ClassACM" e di altre classi eventualmente sviluppate.

NOTA:

- **Il formato dei file ACM deve essere identico per tutti gli alunni (si veda esempio allegato).**
- **Il programma deve essere realizzato rigorosamente ad oggetti progettando una o più classi (si veda esempio allegato).**
- **L'esempio fornito utilizza come algoritmo di cifratura AES (Advanced Encryption Standard).**
- **L'esempio fornito consente la cifratura solo di file di testo.**
- **L'applicazione deve "ricordare" l'ultima directory di input e di output utilizzata (usare file di configurazione o registri).**