

# Sistemi Operativi: Laboratorio

## Specifica Progetto Giugno/Luglio 2021

L'obiettivo del progetto è sviluppare una semplice applicazione che consenta di cifrare file utilizzando una variante del *Cifrario di Vernam*, qui denominato *bvernan*. L'algoritmo proposto sfrutta una semplice proprietà dell'operatore binario *XOR*:

$$(A \text{ XOR } B) \text{ XOR } B = A$$

Data una sequenza di *k*-byte  $b_0 \dots b_{k-1}$  (detta chiave) la funzione di codifica di una sequenza di byte  $d_0 \dots d_N$  la funzione di *codifica/decodifica* segue il seguente semplice procedimento.

La sequenza  $d_0 \dots d_N$  viene per prima cosa suddivisa in  $\frac{N}{k}$  blocchi (divisione intera),  $D_0, \dots, D_{\left(\frac{N}{k}-1\right)}$  ognuno dei quali consiste di esattamente *k* byte (a parte l'ultima sequenza che, ovviamente, potrà contenere un numero inferiore di byte).

Successivamente ogni sequenza  $D_j = d_{j,0} \dots d_{j,k-1}$  viene trasformata nella sequenza  $D'_j = d'_{j,0} \dots d'_{j,k-1}$  tale che per ogni *i*:

$$d'_{j,i} = b_{(j+i) \bmod k} \text{ XOR } d_{j,i}$$

Ossia il byte in posizione *i* del blocco *j* viene messo in *XOR* con il byte  $(j+i) \bmod k$  della chiave.

La sequenza di output verrà quindi ottenuta dalla giustapposizione delle sequenze  $D'_0, \dots, D'_{\left(\frac{N}{k}-1\right)}$ .

Sviluppare l'applicazione *bvernan* che riceve come parametri:

- Il file usato come chiave (*keyfile*);
- Il file da elaborare (*inputfile*);
- Il file di output (*outputfile*).

Invocato con il seguenti parametri:

```
bvernan keyfile inputfile outputfile
```

Il progetto verrà valutato secondo i seguenti parametri:

1. Uso di *make* o di *CMake*;
2. Organizzazione del codice e strutture dati utilizzate;
3. Coerenza con le specifiche date;
4. Capacità di gestire file di dimensioni crescenti;
5. Tempi di esecuzione.

Il progetto dovrà essere consegnato in un archivio *.zip*, *.tgz* o *.tar.gz*, contenente la sola cartella chiamata *<Nome><Cognome><Matricola>* (ad esempio MariaBianchi098765).

**L'uso di formati diversi da quelli consentiti comporterà la NON VALUTAZIONE del progetto.**