



A Huffman Code Based Crypto-System

A cura di
Prof. Bruno Carpentieri

Paolo Labanca
Maria Giovanna Albanese
Manuel Flora

INDICE

1 Introduzione

2 Codifica di Huffman

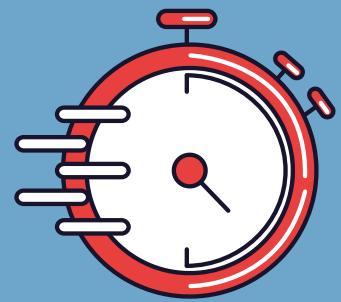
3 Trasformazioni

4 Sicurezza

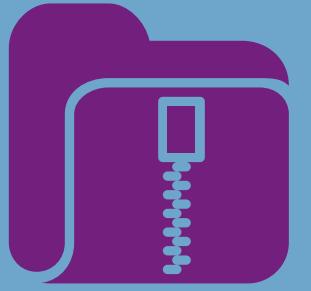
5 Risultati

INTRODUZIONE

Problemi di comunicazione sulla rete:



Velocità di elaborazione:
il trasferimento dei dati attraverso la rete viene modificato dalla velocità della rete



Risparmio di spazio sui dati:
Ridurre la dimensione del file trasformati

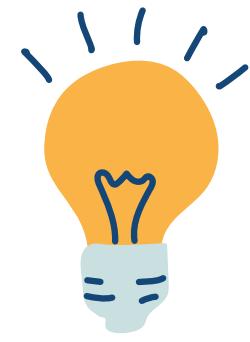


Sicurezza:
Proteggere le informazioni da possibili attacchi



INTRODUZIONE

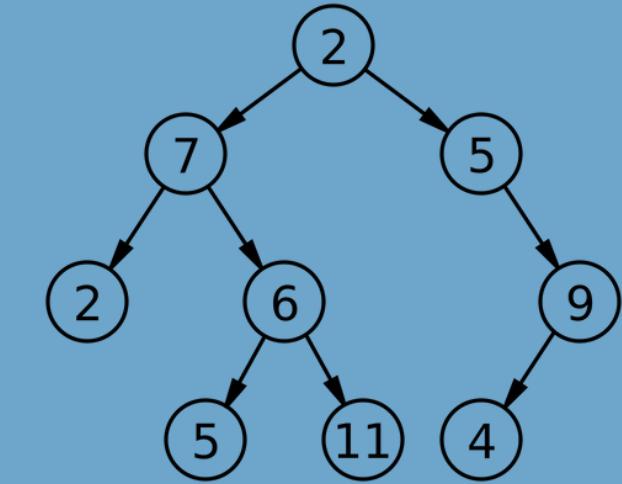
Le due componenti fondamentali sono:



**Crittosistemi
di compressione**

CRITTOSISTEMA BASATO SU HUFFMAN

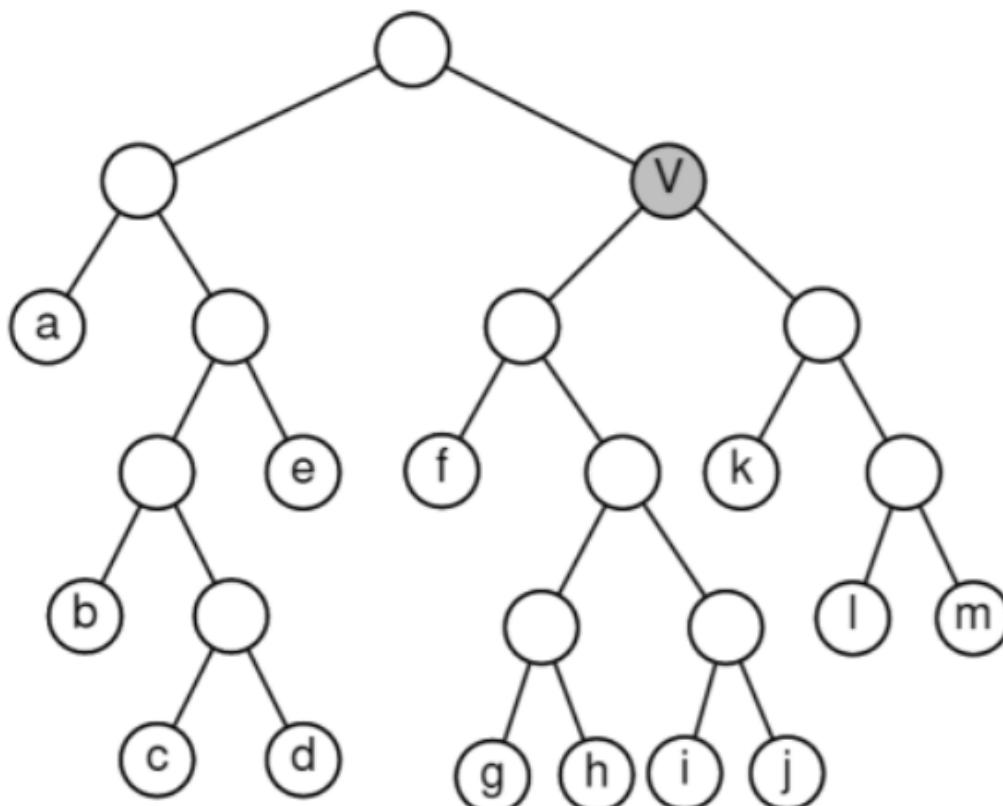
Inizializzazione dell'albero di Huffman



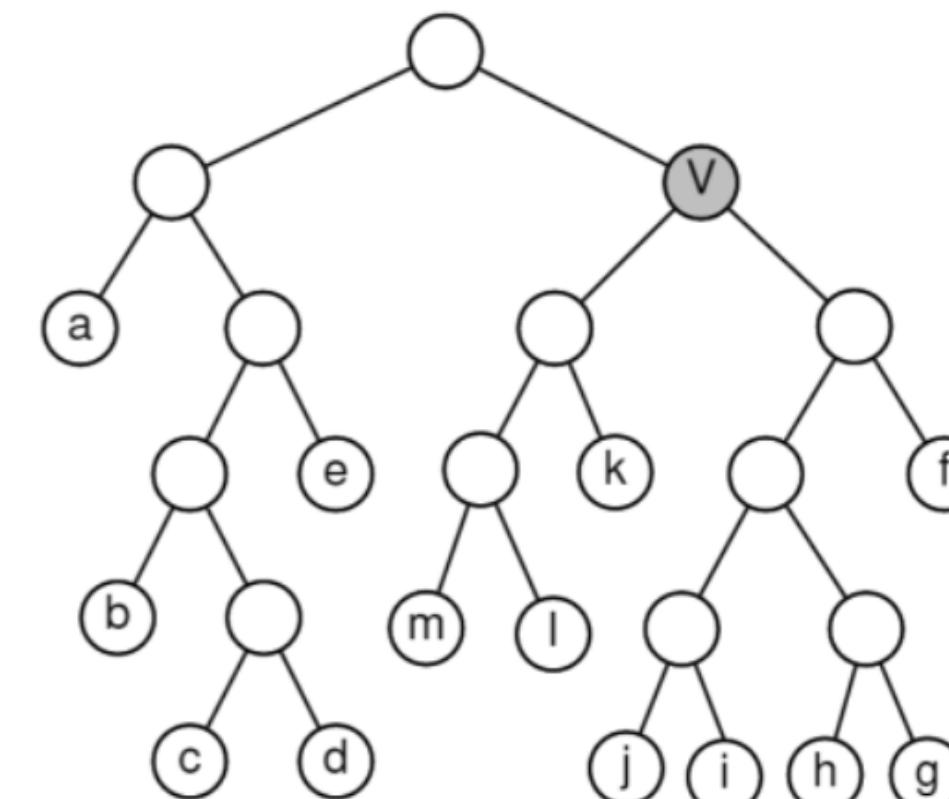
- Utilizzare una chiave segreta pseudo-casuale per selezionare un nodo interno V
- Applicare le trasformazione in modo pseudo-casuale
- Chiavi diverse hanno output diversi ma con lo stesso rapporto di compressione

TRASFORMAZIONE: MIRROR

10110 (leaf i) $\Rightarrow \overline{10110} = 11001$



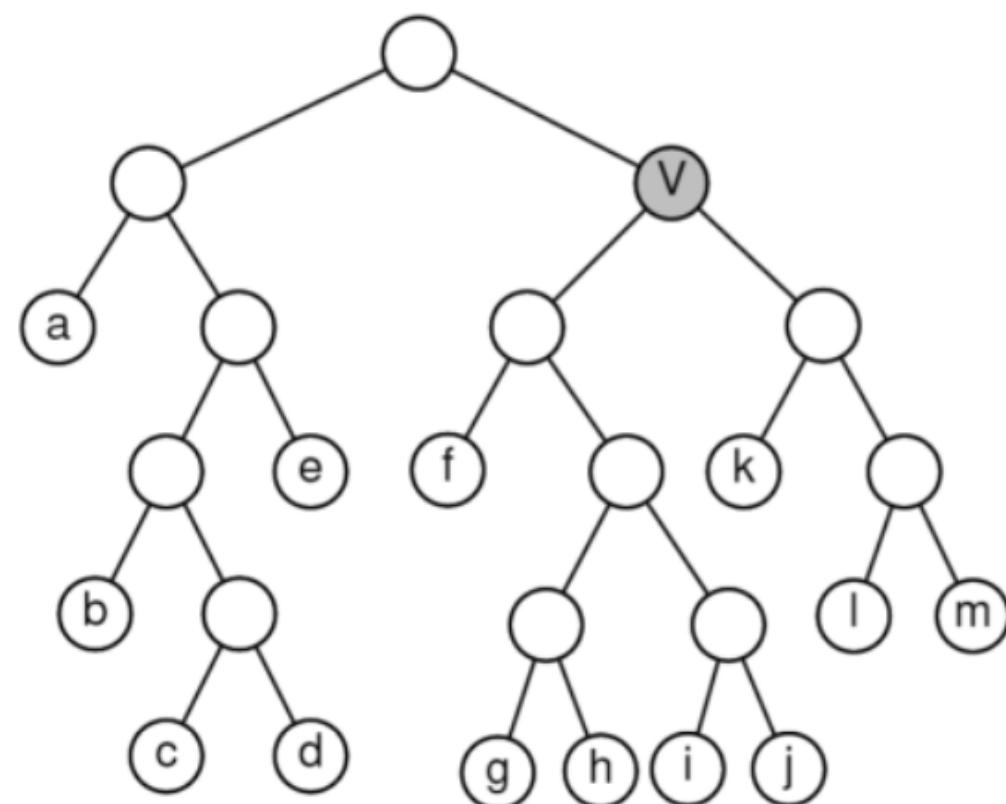
Original



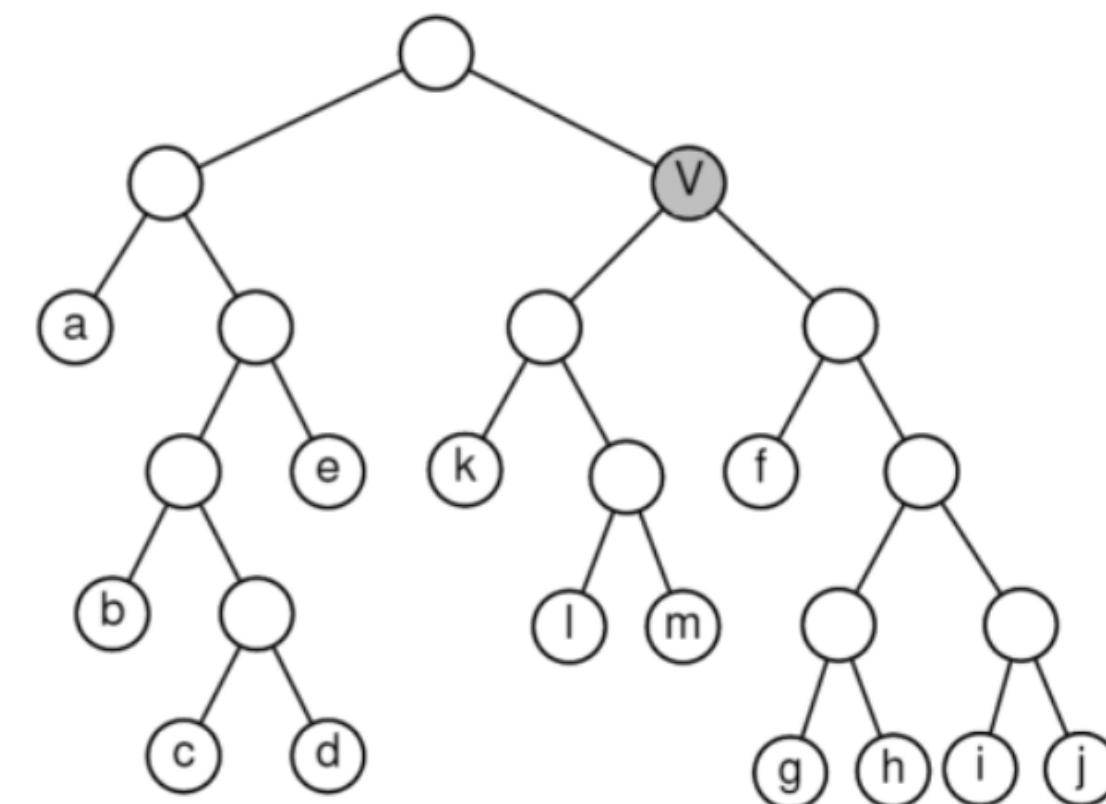
Mirror

TRASFORMAZIONE: SWAP

10110 (leaf i) \Rightarrow $1\bar{0}110 = 11110$

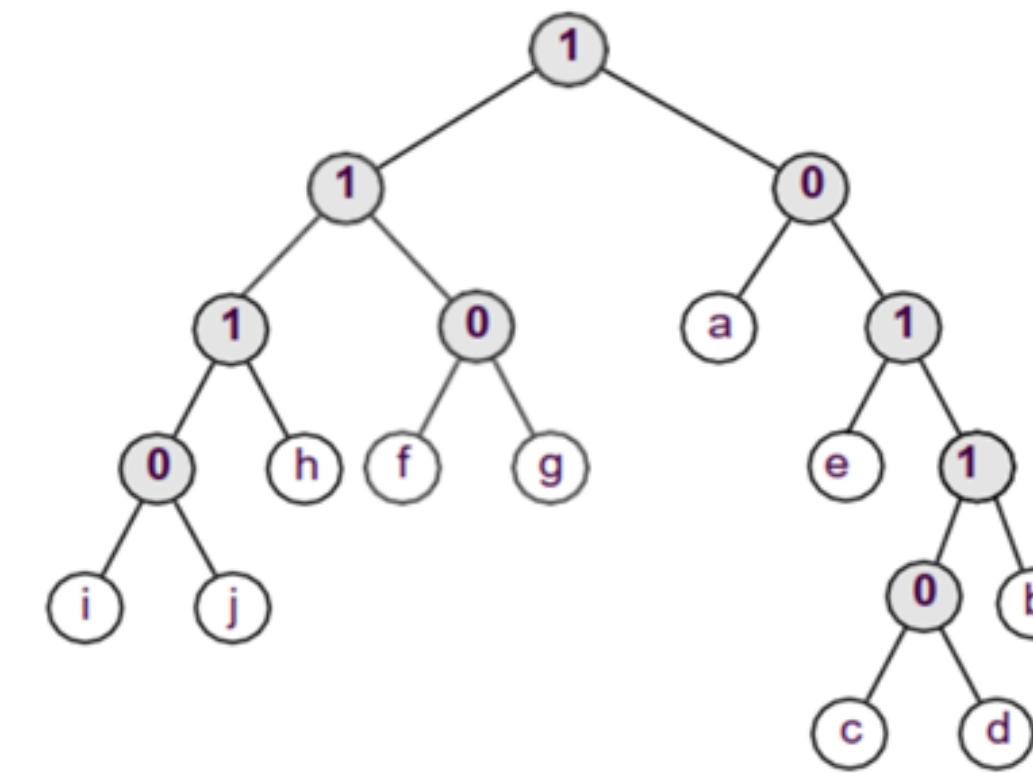
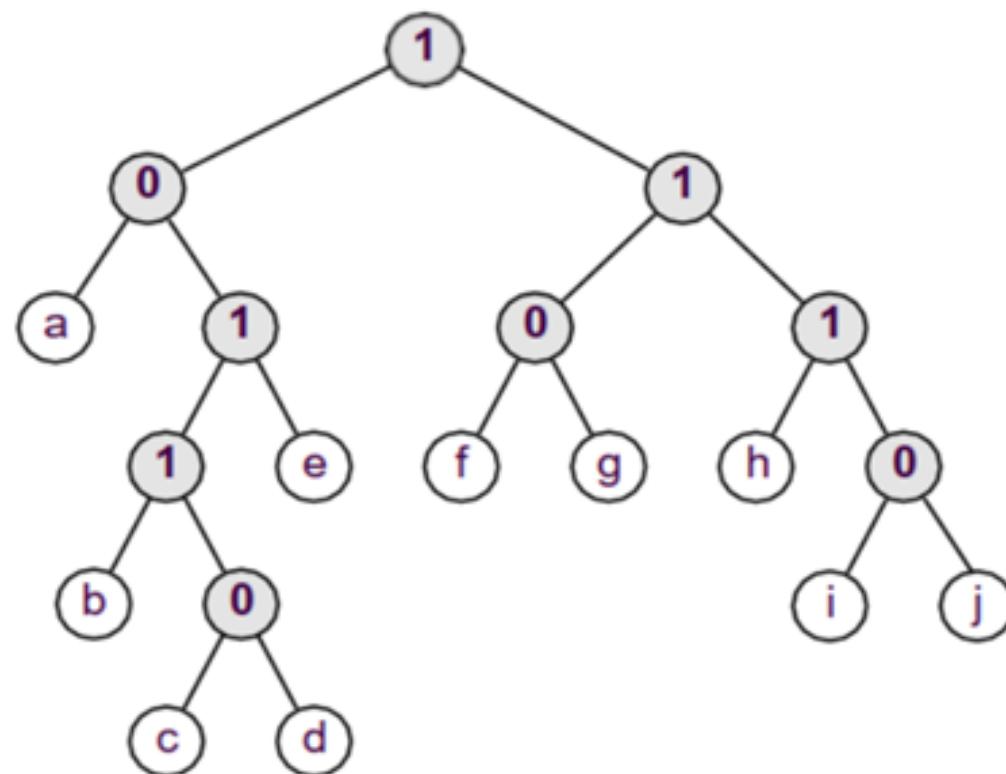


Original



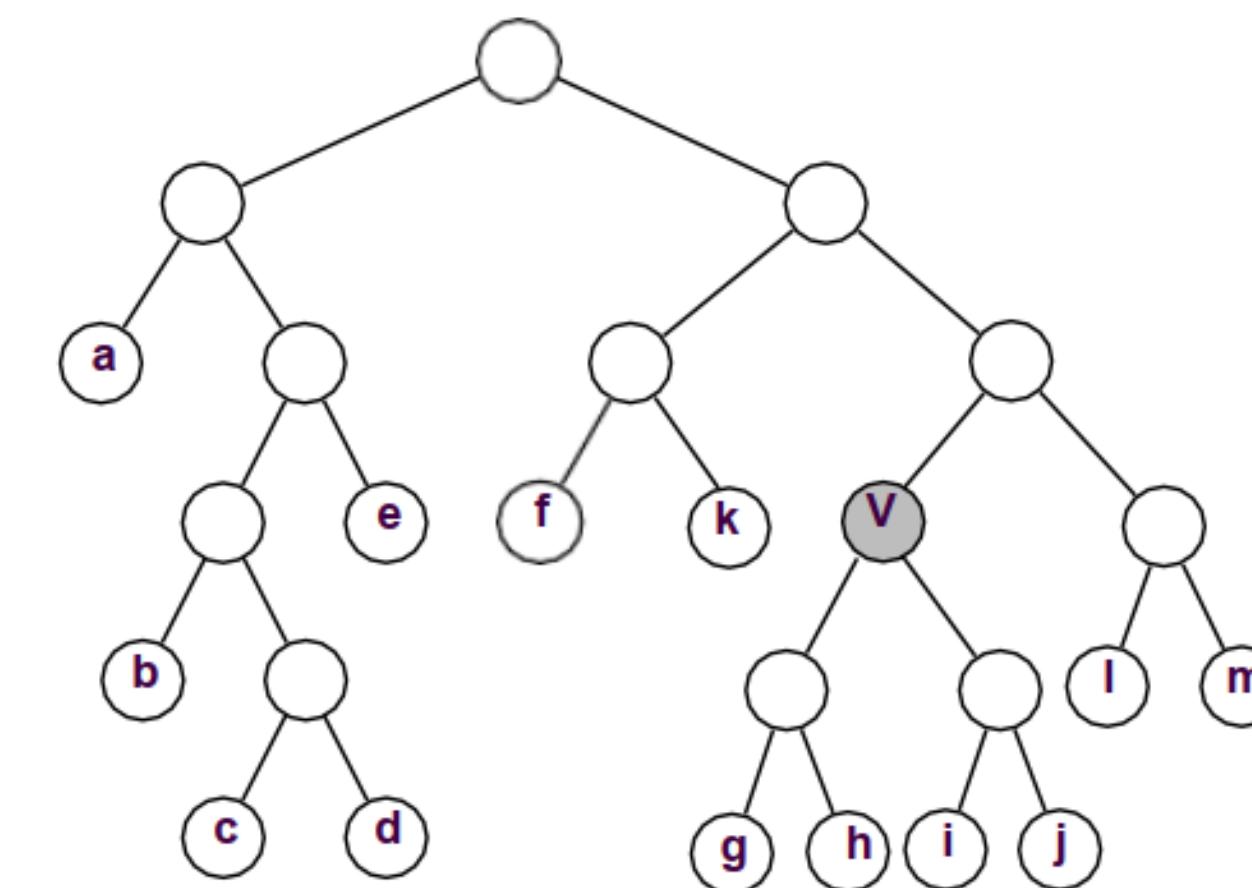
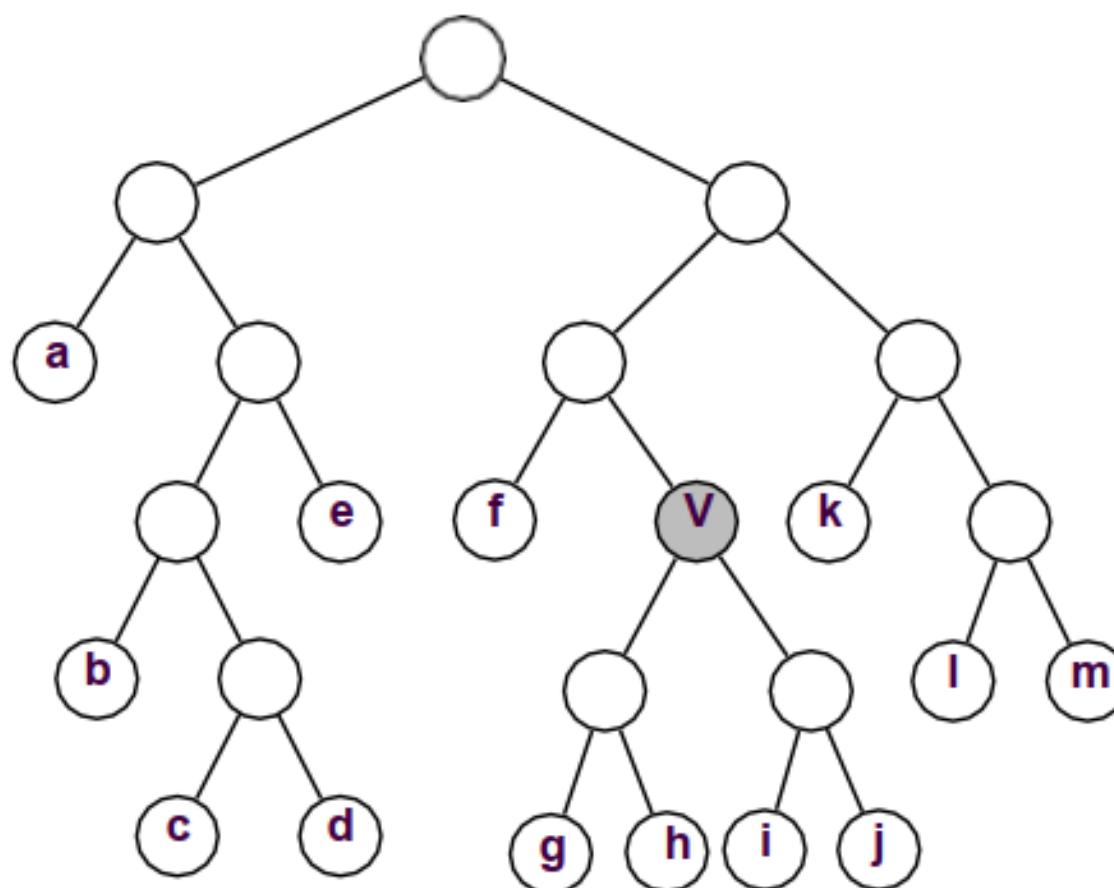
Swap

TRASFORMAZIONE: BULK-CRYPTO-HUFFMAN



TRASFORMAZIONE: LEVEL-SWAP

10110 (leaf i) => **11010.**



SICUREZZA



- L'obiettivo della crittografia è nascondere il contenuto di un determinato file di testo in chiaro da un intercettatore non autorizzato.
- L'obiettivo di un avversario è provare a infrangere il codice.

SICUREZZA



- Applicare N trasformazioni pseudo-casuali sull'albero di Huffman
- L'avversario conosce i dettagli del processo, tranne: le chiavi segrete e il PAD
- Questo rende difficile la decifratura e la decompressione

ATTACCHI CPA

OBIETTIVO: Stessa chiave segreta, testi cifrati diversi

- Aggiungere un PAD pseudo-casuale con lunghezza fissata
- Il decoder elimina prima il PAD



RISULTATI

DATA SET

Large Corpus tratto dall'opera 'Canterbury' in bible.txt,
versione di The King James, con dimensione :
4,047,392 Bytes



INDISTINGUIBILITÀ

| bit-string | m-m-s | BCH-BCH-ls | ls-ls-BCH |
|------------|---------|------------|-----------|
| 0 | 0.47251 | 0.47232 | 0.47232 |
| 1 | 0.52749 | 0.52768 | 0.52768 |
| 00 | 0.15259 | 0.15261 | 0.15272 |
| 01 | 0.25526 | 0.25533 | 0.25471 |
| 10 | 0.25526 | 0.25533 | 0.25423 |
| 11 | 0.18269 | 0.17986 | 0.17921 |
| 000 | 0.05976 | 0.05966 | 0.05921 |
| 001 | 0.13147 | 0.13208 | 0.13308 |
| 010 | 0.09228 | 0.09390 | 0.09400 |
| 011 | 0.13990 | 0.13859 | 0.13729 |
| 100 | 0.13147 | 0.13208 | 0.13238 |
| 101 | 0.09953 | 0.10015 | 0.10039 |
| 110 | 0.13990 | 0.13859 | 0.13839 |
| 111 | 0.07525 | 0.07752 | 0.07800 |

m=Mirror, s=Swap, BCH= Bulk-Crypto-Huffman, ls=Level swap

CONFRONTO RISULTATI

| bit-string | mix | L-Swap | Mirror | Swap | Bulk |
|------------|----------------|----------|----------|----------|----------|
| 0 | 0.52749 | 0.500097 | 0.500061 | 0.500138 | 0.500034 |
| 1 | 0.47251 | 0.499903 | 0.499939 | 0.499862 | 0.499966 |
| 00 | 0.15259 | 0.250076 | 0.249985 | 0.250074 | 0.250060 |
| 01 | 0.25526 | 0.250021 | 0.250076 | 0.250074 | 0.249974 |
| 10 | 0.25526 | 0.250021 | 0.250076 | 0.250074 | 0.249974 |
| 11 | 0.18269 | 0.249882 | 0.249863 | 0.249798 | 0.249992 |
| 000 | 0.05976 | 0.121652 | 0.124964 | 0.125050 | 0.125053 |
| 001 | 0.13147 | 0.128424 | 0.125022 | 0.125024 | 0.125007 |
| 010 | 0.09228 | 0.121522 | 0.125012 | 0.124975 | 0.124968 |
| 011 | 0.13990 | 0.128499 | 0.125063 | 0.125089 | 0.125007 |
| 100 | 0.13147 | 0.128424 | 0.125022 | 0.125024 | 0.125007 |
| 101 | 0.09953 | 0.121597 | 0.125054 | 0.125040 | 0.124967 |
| 110 | 0.13990 | 0.128499 | 0.125063 | 0.125089 | 0.125007 |
| 111 | 0.07525 | 0.121384 | 0.124800 | 0.124709 | 0.124985 |

SICUREZZA CPA CON NHD

$$NHD(A, B) = \frac{1}{n} \sum_{i=1}^n a_i XOR b_i$$

Il valore ottenuto dal file in input è 0.4060802



**GRAZIE
PER L'ATTENZIONE**