Freezing Video

Tema d'anno 2016/2017
Corso di Data Security
Prof. Ing. G. Mastronardi

Studenti
G. Allegretta
F. Scarangella

Scaletta

- Crittografia
- DRM
- Freezing Video

Crittografia

Unione di due parole greche:
κρυπτός (*kryptós*) che significa "nascosto"
γραφία (*graphía*) che significa "scrittura"

La crittografia si ottiene applicando al testo in chiaro una funzione matematica, chiamata algoritmo di codifica, che utilizza una chiave. Quello che si ottiene è un testo incomprensibile e indecifrabile da chi non conosce la chiave.

In un sistema crittografico è importante tener segreta la chiave, non l'algoritmo di crittazione.

Principio di Kerchoffs

Requisiti

- **Riservatezza**
  Comunicazione riconosciuta solo dal destinatario
- **Integrità dei dati**
  Il documento trasmesso non deve subire alcun tipo di alterazione
- **Autenticità**
  Riconducibilità al mittente
- **Non ripudio**
  Non disconoscimento da parte del mittente
- **Facilità di utilizzo**

Metodi

Chiave pubblica-privata

Chiamata anche crittografia a chiave asimmetrica.

Vengono utilizzate due chiavi distinte: la chiave pubblica e la chiave privata.

Le due chiavi sono complementari nel processo di comunicazione, ma la conoscenza della chiave pubblica non consente di risalire alla chiave privata.

Chiave segreta

Chiamata anche crittografia a chiave simmetrica.

Viene utilizzata un'unica chiave, sia per la cifratura che per la decifratura.

In questo caso ci si pone il problema dello scambio della chiave tramite un canale sicuro.

Principi

Confusione

La relazione tra chiave e testo cifrato è quanto più complessa e non correlata possibile.
Non si può risalire ad essa a partire dal testo cifrato.

C'è corrispondenza tra lettere della trasformazione.

Diffusione

L'algoritmo distribuisce le correlazioni statistiche del testo lungo tutto l'alfabeto usato per la cifratura.

Non conserva la corrispondenza tra lettere della trasformazione, causando problemi per la ricostruzione del messaggio.

ESEMPI
Solo confusione: la modifica di un carattere del messaggio in chiaro crea la modifica di un solo carattere del messaggio cifrato
Solo diffusione: la modifica di un carattere in chiaro crea la modifica di più di un carattere del messaggio cifrato

AES-128

Algoritmo di cifratura a blocchi utilizzato come standard dal governo degli Stati Uniti d'America.

Rappresenta un’evoluzione del Data Encryption Standard (DES) che ha perso efficacia per vulnerabilità intrinseche.

Procedimento

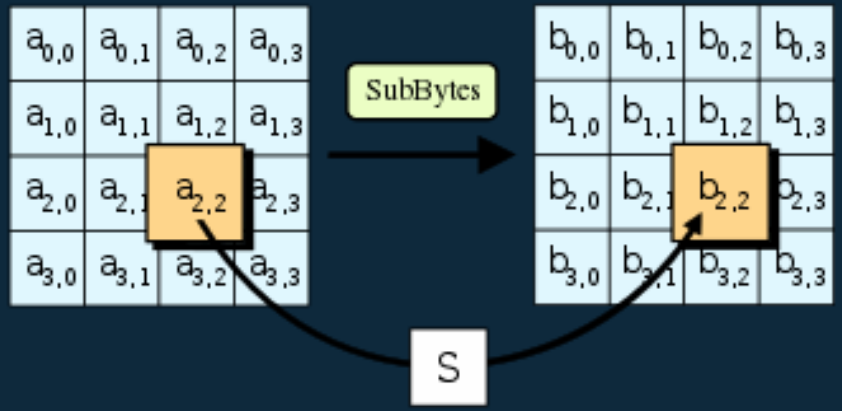
Utilizza un blocco a dimensione fissa di 128 bit, una chiave di 128 bit e delle matrici 4x4 byte chiamate «State».

Inizialmente, si esegue il passaggio chiamato AddRoundKey.
Poi è prevista l'esecuzione di 10 «round»*, composti dai seguenti passaggi:

*L'ultimo «round» salta il passaggio MixColumns

SubBytes

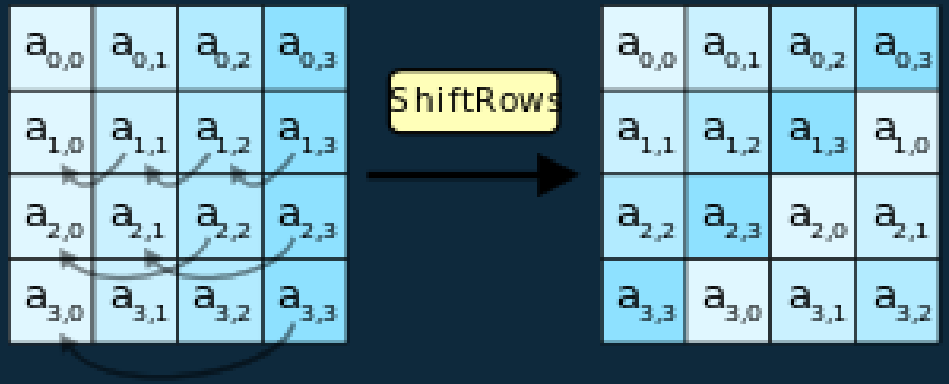
Tutti i byte della matrice sono modificati tramite una S-box ad 8 bit. La S-box è una tabella di sostituzione scelta in modo da creare sostituzioni non lineari.



Le S-box vengono utilizzate per oscurare le relazioni tra il testo in chiaro e quello cifrato.
Realizzano il principio di confusione enunciato da Shannon.

ShiftRows

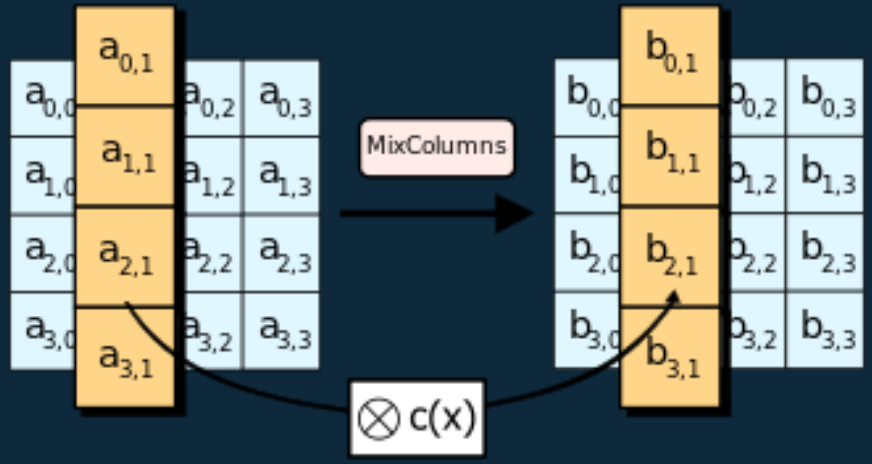
Tutti i byte sono spostati di un certo numero di posizioni dipendente dalla riga di appartenenza.
La prima riga resta invariata, la seconda viene spostata di un posto verso sinistra, la terza è spostata di due posti e la quarta di tre.



L'ultima colonna dei dati in ingresso andrà a formare la diagonale secondaria della matrice in uscita

MixColumns

I 4 byte di ogni colonna vengono combinati con una trasformazione lineare invertibile.

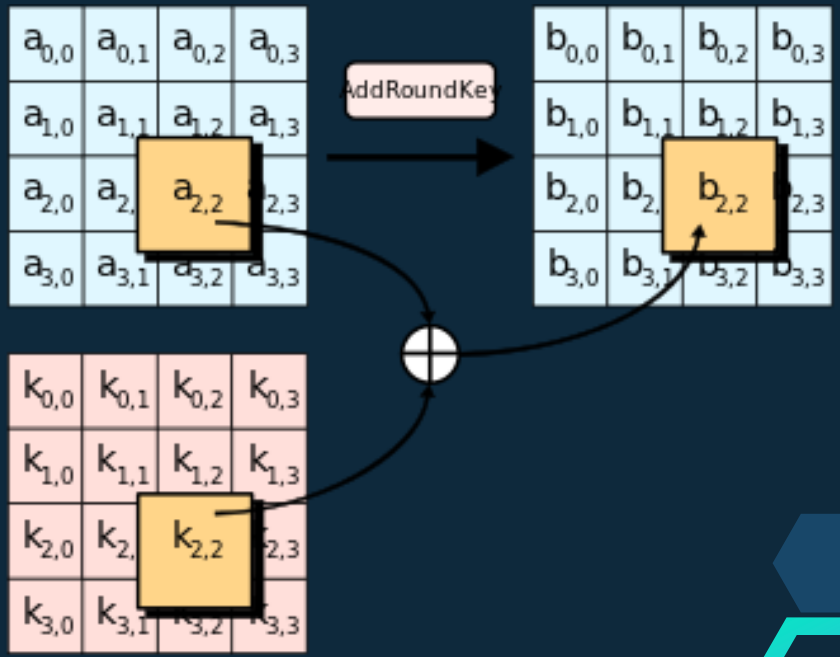


I passaggi «ShiftRows» e «MixColumns» realizzano il principio di diffusione enunciato da Shannon.

AddRoundKey

Ogni byte della tabella viene combinato tramite l'operazione logica XOR con la chiave di sessione.

La chiave di sessione viene ricavata dalla chiave primaria ad ogni round dal gestore delle chiavi.



DRM (Digital Rights Management)

Indica i sistemi tecnologici mediante i quali i titolari di diritto d'autore (e dei diritti connessi) possono tutelare, esercitare ed amministrare tali diritti nell'ambiente digitale.

Funzionamento

I file audio/video vengono codificati e criptati in modo da garantire la protezione contro la copia e la diffusione non autorizzata.
Viene consentito un uso limitato (nel tempo o nell'utilizzo) e definito dalla licenza fornita.

Il procedimento maggiormente impiegato è la segmentazione.

FFmpeg

Rappresenta il framework multimediale di riferimento.

È in grado di:

- Codificare, decodificare e transcodificare
- Muxare e demuxare i flussi video e audio
- Filtare e riprodurre qualsiasi file multimediale
- Realizza la segmentazione

È una dipendenza fondamentale del nostro progetto

3

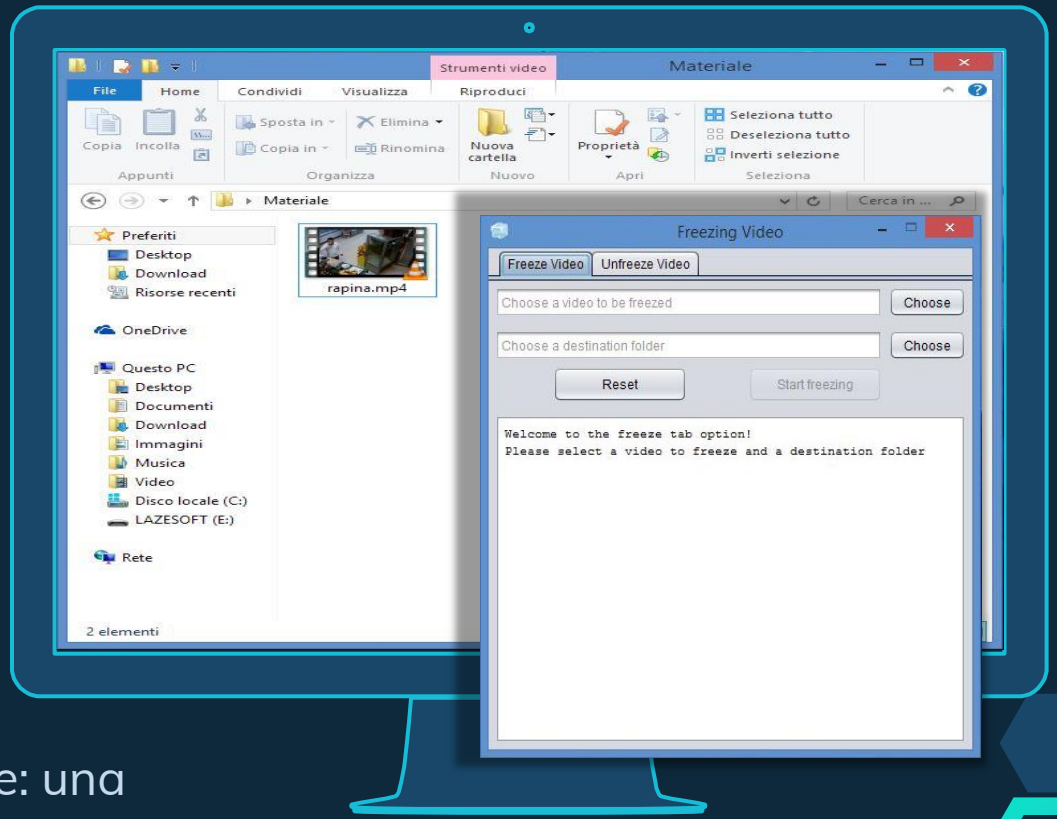
Come congelare una prova?
Freezing Video

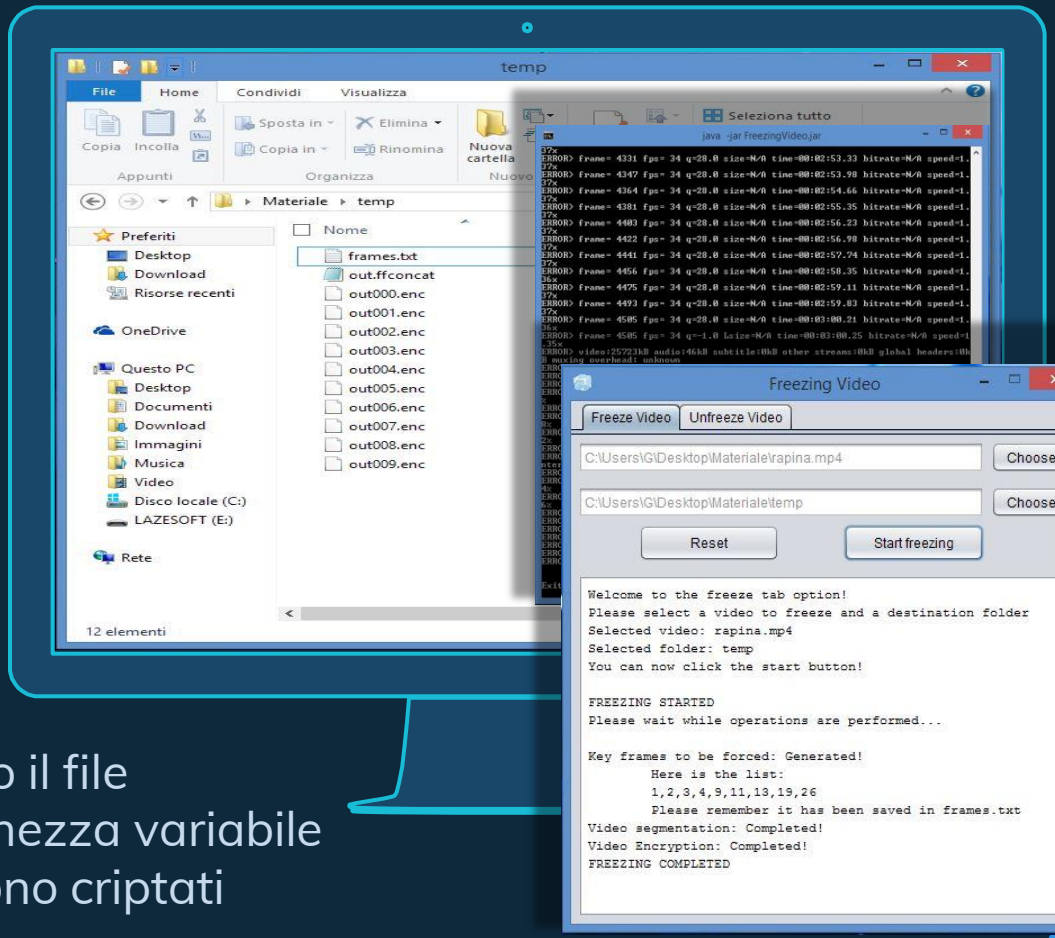
Cartella sorgente

All’interno di questa cartella vi è il file multimediale da congelare

Software Freezing Video

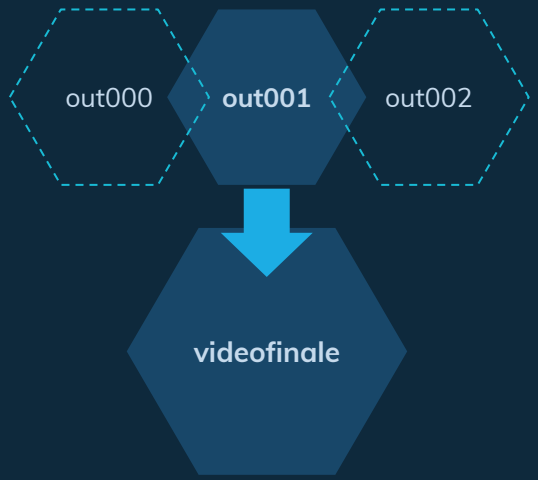
All’avvio si hanno due schede: una consente di congelare il file mentre l’altra di effettuare l’operazione inversa

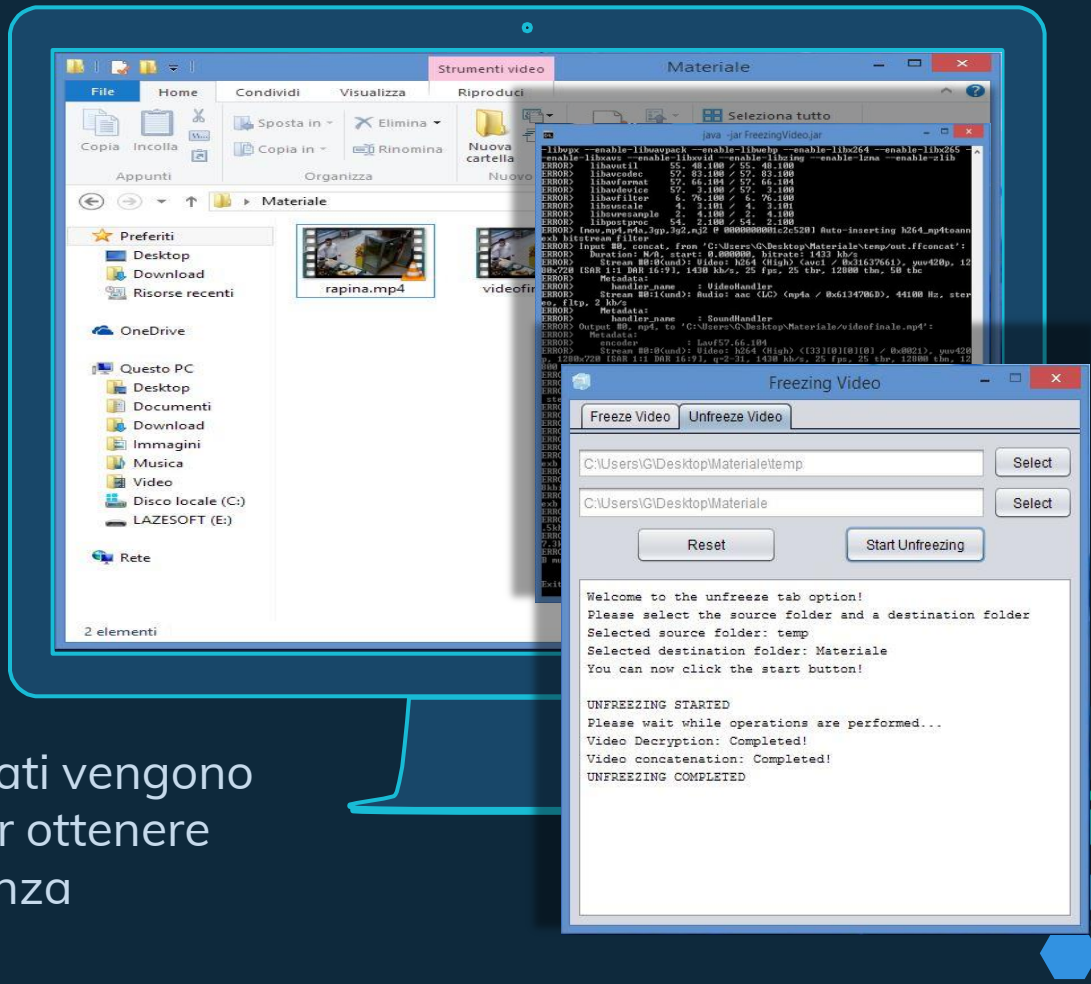




Cartella temp (1/2)

In questa cartella viene diviso il file sorgente in segmenti di lunghezza variabile che, successivamente, vengono criptati





Cartella temp (2/2)

I file precedentemente generati vengono decriptati e desegmentati per ottenere nuovamente il video di partenza

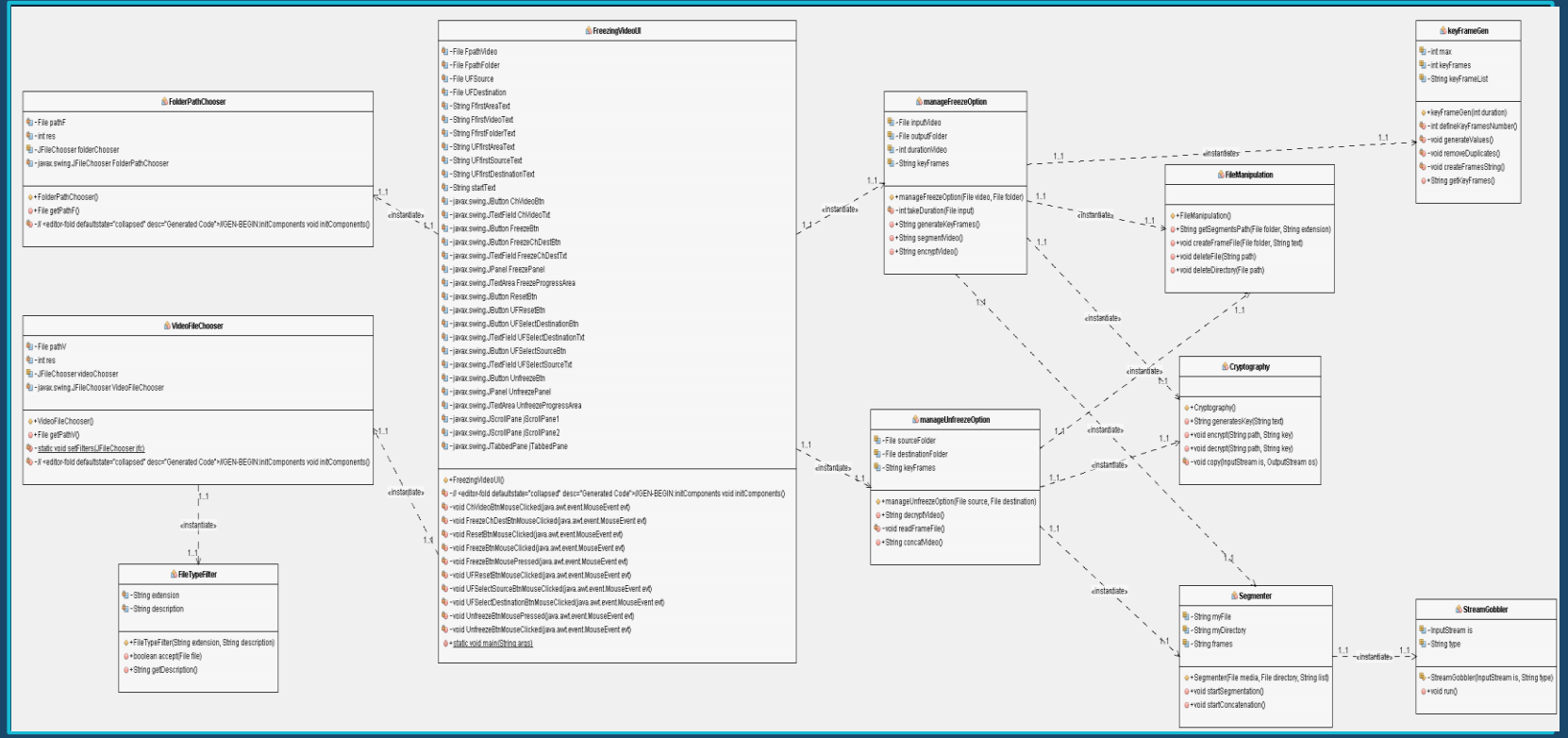


Diagramma UML

Conclusioni

“Freezing video” è un software completo e funzionante.

Nonostante ciò è possibile aumentare la complessità del sistema attraverso alcuni accorgimenti quali:

- Nomi più complessi da assegnare ai segmenti
- Algoritmo di criptazione più sicuro (es. AES-256)
- Possibilità di condivisione delle chiavi direttamente dal programma

Grazie per l’attenzione!

Studenti

- G. Allegretta
- F. Scarangella