Istituto Tecnico Tecnologico Statale "Fedi-Fermi" - Pistoia

LABORATORIO DI TECNOLOGIE INFORMATICHE

a.s. 2020/2021

Gruppo 5 IA07

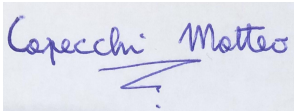
Nomi dei componenti del gruppo Bresci Bernardo, Capecchi Matteo, Timour Ilyas

Titolo Esercitazione JAVA-Cifrature Semplici

Data Inizio 24/10/2021

Data	Ore	Luogo	Nomi dei componenti del gruppo
24.10.2021	2	SCUOLA	Bresci Bernardo, Capecchi Matteo, Timour Ilyas
24.10.2021	3	CASA	Bresci Bernardo, Capecchi Matteo, Timour Ilyas
24.10.2021	2	SCUOLA	Bresci Bernardo, Capecchi Matteo, Timour Ilyas
24.10.2021	1	CASA	Bresci Bernardo, Capecchi Matteo, Timour Ilyas
24.10.2021	2	SCUOLA	Bresci Bernardo, Capecchi Matteo, Timour Ilyas
24.10.2021	3	CASA	Bresci Bernardo, Capecchi Matteo, Timour Ilyas

Data Consegna 24.11.2021



Sommario

Problema

Titolo esperienza

JAVA-cifrature semplici

Testo del problema

Utilizzando JAVA e le socket UDP si implementi un semplice sistema di messaggistica con cifratura. Le applicazioni da sviluppare sono due:

SECRET SENDER:

Utilizzata da più agenti segreti, l'applicazione dovrà prevedere la possibilità di:

• Inserire un testo (massimo 512 caratteri)

• Inserire un codice numerico di 4 cifre dell'agente segreto

• Cifrare il messaggio (codice agente+": "+ testo) con il cifrario di Cesare o quello di Vigenère a scelta

• Inviare il messaggio ad una SECRET INBOX di cui si dovrà specificare IP e PORTA.

Nota: Le chiavi di cifratura (un numero nel caso di Cesare, una parola di 5 caratteri nel caso di Vigenère) potranno essere cambiate ad ogni invio attraverso l'interfaccia grafica.

SECRET INBOX:

Utilizzata dal quartier generale delle spie, la SECRET INBOX dovrà ricevere, salvare e visualizzare uno storico dei messaggi ricevuti con la possibilità di decifrarli singolarmente scegliendo l'algoritmo e la chiave di cifratura.

OPZIONALE:

Si provi a realizzare un'opzione BRUTE FORCE che tenti in maniera esaustiva di rompere la cifratura. Come condizione per il (possibile) successo della forzatura, si utilizzi il vincolo che i primi 4 caratteri del messaggio devono essere cifre numeriche seguite da ": ".

Scopo

Utilizzando JAVA e le socket UDP si implementi un semplice sistema di messaggistica con cifratura.

Ritorna al sommario

Cenni Teorici

Cifrario di cesare = È un cifrario a sostituzione monoalfabetica, in cui ogni lettera del testo in chiaro è sostituita, nel testo cifrato, dalla lettera che si trova un certo numero di posizioni dopo nell'alfabeto. La sostituzione avviene lettera per lettera, scorrendo il testo dall'inizio alla fine.

Il cifrario di Vigenère = è il più semplice dei cifrari polialfabetici Si basa sull'uso di un versetto per controllare l'alternanza degli alfabeti di sostituzione. Invece di spostare sempre dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile ma ripetuto, determinato in base ad una parola chiave, da concordarsi tra mittente e destinatario, e da scrivere ripetutamente sotto il messaggio, carattere per carattere; la chiave era detta anche verme, per il motivo che, essendo in genere molto più corta del messaggio, deve essere ripetuta molte volte sotto questo.

Un cifrario, nella crittografia, è un algoritmo utilizzato per eseguire operazioni o una serie di passaggi ben definiti che possono essere seguiti come una procedura, volte a rendere *oscuro*, ossia semanticamente non leggibile, un testo di un messaggio in chiaro (*plain text*) o, al contrario, al ripristino in chiaro di un messaggio precedentemente cifrato.

Linguaggi assimilati

Programmazione del linguaggio Java (eclipse)

Ritorna al sommario

Analisi del problema

Dovevamo realizzare due applicazioni che riescano a cifrare dei messaggi tramite due modi:

Secret sender = Inserire un testo (massimo 512 caratteri)

Inserire un codice numerico di 4 cifre dell'agente segreto

Cifrare il messaggio (codice agente+": "+ testo) con il cifrario di

Cesare o quello di Vigenère a scelta

Inviare il messaggio ad una SECRET INBOX di cui si dovrà

specificare IP e PORTA.

Secret inbox = dovrà ricevere, salvare e visualizzare uno storico dei messaggi ricevuti con la possibilità di decifrare singolarmente scegliendo l'algoritmo e la chiave di cifratura.

Dati di ingresso/uscita

Secret server:

I= Messaggio da cifrare

O= Messaggio cifrato

Secret inbox:

I= Messaggio cifrato

O= Messaggio decifrato

Vincoli aggiuntivi

Nessun vincolo aggiuntivo

Ritorna al sommario

Ipotesi risolutiva

Ritorna al sommario

Funzioni espletate del programma

Ambiente di sviluppo

Eclipse (JAVA)

Librerie utilizzate

Listato del codice

Ritorna al sommario

Manuale per l’utente

Utilizzare un ide java o una java virtual machine per avviare i programmi.

Videata del codice

Ritorna al sommario

Spiegazione per l’utente

Per eseguire entrambe i programmi tramite i file eseguibili, l'utente dovrà avere una Java Virtual Machine aggiornata ad una versione recente e quindi non obsoleta, ed avviare entrambi gli eseguibili tramite la Java Virtual Machine.

Requisiti minimi

Istruzioni per utilizzo

Aprire il file .java con il programma eclipse e seguire le istruzioni del programma.

Bibliografia – Sitografia di riferimento

CIFRATURA

CIFRATURA DI CESARE

CIFRATURA DI VIGENÈRE

Ritorna al sommario

Osservazioni e conclusioni personali

Grazie ad alcuni aiuti e una buona spiegazione da parte del professor Giusti e comprensione del problema siamo riusciti a realizzare il programma. Non nascondiamo che abbiamo durato molta fatica per creare questo progetto, dato che tutti e due non siamo proprio degli esperti della programmazione java, siamo riusciti a fare il programma. Inoltre abbiamo riscontrato una maggiore sintonia cambiando il proprio gruppo rispetto al primo progetto e siamo riusciti così a lavorare al cento per cento delle nostre possibilità.

RITORNA AL SOMMARIO