Cifrature per il Cloud

Prototipo ABE-SE: Manuale Utente

Compilazione:	**E. Bellini**
Verifica:	**-**
Approvazione:	**-**
Data creazione:	**26/08/2015**
Livello di Classifica:	**NON CLASSIFICATO**
Data Ultima Modifica:	**03/11/2016**
ID documento:	**ID**
Versione:	**1.0**
Numero pagine:	**46**
ID progetto:	**000**
Priorità progetto:	**None**
File:	**abe_se_proto**

Indice

Versione

Data	*Versione*	*Nome file*	*Descrizione*
03/11/2016	1.0	abe_se_proto	Rilascio iniziale

Acronimi e abbreviazioni

ABE	Attribute Based Encription
MLS	Multi-Level Security
VPSS	Virtual Private Secure Server

1 Introduzione

Uno dei principali scopi del progetto è la definizione di un'architettura Virtual Private Secure Server (VPSS) che integri funzionalità di Multi-Level Security (MLS) e di *Searchable Encryption*. Èstata realizzata anche un'implementazione software dimostrativa (**Dimostratore VPSS**, versione **1.0**, di cui questo documento costituisce la descrizione ed il manuale d'uso.
Dato il fine dimostrativo, lo sviluppo del software è stato focalizzato su elementi innovativi come Attribute-Based Encryption e Searchable Encryption, non curandosi di altri aspetti che, per quanto fondamentali in un sistema di sicurezza completo, sono qui di scarso interesse e renderebbero inutilmente macchinoso l'utilizzo del Dimostratore. Di conseguenza funzioni tipiche del sistema operativo, quali l'identificazione degli utenti al login e la separazione delle loro aree di storage, sono state implementate con meccanismi elementari e più pratici, benché privi di effettiva sicurezza.
Analogamente è offerta per semplicità la possibilità di mantenere sulla stessa macchina tutte le entità previste dal sistema: un'Authority , gli Utenti, un Server di Archiviazione e un Server di Ricerca (si veda 2.3). E' tuttavia immaginabile che questo non sia il caso in un'ipotetica realizzazione concreta di quanto descritto[1], nella quale verosimilmente l'Authority sarebbe implementata su una macchina dedicata *trusted*, gli utenti su client individuali, il Server di Ricerca su una macchina non necessariamente *trusted* e infine il Server di Archiviazione su un servizio di Cloud.
Il Dimostratore è stato realizzato integrando librerie di pubblico dominio con codice appositamente sviluppato, prevalentemente nei linguaggi C e Python, ed è installabile sia in ambiente Windows sia in ambiente Linux. Una volta installato fornisce un Client che permette di simulare l'attività sia degli utenti sia dell'Authority.

1.1 Organizzazione del documento

Il documento è così organizzato:

- il Capitolo 2 fornisce una descrizione sintetica dell'architettura generale del sistemaVPSS;
- il Capitolo 3 descrive la procedura di installazione del Dimostratore per Windows Seven e per Linux (Ubuntu 14.04);
- il Capitolo 4 ne descrive invece la procedura di inizializzazione;
- il Capitolo 5 ne descrive l'utilizzo a regime;
- il Capitolo 6 è infine dedicato alla descrizione dettagliata degli oggetti crittografici utilizzati e del loro formato.

[1] In ogni caso il Dimostratore consente di porre i server su macchine distinte.

2 Architettura generale

In questo capitolo viene fornita una descrizione schematica del Dimostratore VPSS. Innanzitutto ne viene ricordato lo scenario di utilizzo, poi, dopo aver rapidamente ricordato le caratteristiche della ciphertext-policy Attribute Based Encription (ABE) (2.2), se ne descrive l'architettura generale. In particolare si definiscono le entità coinvolte nel sistema considerato e si considerano le funzioni di ciascuna di esse.

2.1 Scenario di utilizzo

Descriviamo brevemente l'architettura implementata dal Dimostratore. Essa prevede un insieme di utenti che, avendo accesso ad un'area comune di memorizzazione, possono condividere dati in modo sicuro secondo una logica di MLS, in cui la compartimentazione non viene eseguita a livello fisico ma a livello logico tramite adeguate tecniche crittografiche.
Più precisamente nell'area di memorizzazione, implementata tramite uno specifico Server di Archiviazione, i dati vengono posti in forma cifrata con tecniche ABE. La cifratura utilizzata determina la possibilità di accesso (o meno) di un utente in funzione degli attributi che gli sono stati riconosciuti. Più precisamente, un ente preposto (Authority nel linguaggio ABE) in fase di attivazione riconosce ad ogni utente certi attributi ed in funzione di questi genera e gli assegna una specifica chiave privata (nel seguito *Chiave Segreta di Decifratura ABE*). Tale chiave mette l'utente in grado di decifrare tutti i messaggi cifrati secondo una policy soddisfatta dai suoi attributi. La cifratura avviene invece tramite una chiave pubblica (nel seguito *Chiave Pubblica ABE*), unica in tutto il sistema e comunicata dall'Authority a tutti gli utenti[1].
E' previsto inoltre che sui dati cifrati possa essere eseguita una forma (limitata) di ricerca di parole chiave o altri metadati, appoggiandosi a questo scopo ad un secondo server (Server di Ricerca) sul quale vengono memorizzate, anch'esse in forma cifrata, le parole chiave associate ad ogni file memorizzato sul Server di Archiviazione. Tale associazione viene definita dall'utente generatore dei dati nel momento in cui li condivide salvandone il contenuto del file sul Server di Archiviazione. La cifratura delle parole chiave, che vengono così rese inaccessibili al Server di Ricerca, è ottenuta tramite tecniche simmetriche convenzionali e una chiave (nel seguito *Chiave Segreta di Ricerca*) condivisa tra tutti gli utenti, generata e distribuita dall'Authority. I due server non hanno tra loro alcuna interazione tra loro né alcun accesso ai dati in chiaro.
Per completezza osserviamo infine che, come in ogni schema ABE (si veda 2.2), è prevista anche una *Chiave Master ABE*.
Nello scenario così definito, le funzioni offerte agli utenti sono così le seguenti:

- cifrare e decifrare (in locale);
- caricare file cifrati sul Server di Archiviazione, associandovi parole chiave che vengono invece caricate, in forma cifrata, sul Server di Ricerca;

[1] Si osservi che, come in ogni sistema a chiave asimmetrica, per cifrare un messaggio è sufficiente conoscere la chiave pubblica. La ABE è però caratterizzata dal fatto che tale chiave non è specifica per ogni utente ma è unica nel sistema.

- effettuare ricerche sui file cifrati caricati nel Server di Archiviazione , utilizzando combinazioni di parole chiave cifrate da sottoporre al Server di Ricerca ;
- scaricare file cifrati dal Server di Archiviazione .

Come mostrato in 5.4, nel Dimostratore queste funzioni sono mantenute distinte, allo scopo di evidenziare la separazione concettuale tra le operazioni di

- cifra/decifra, realizzata secondo schemi ABE (integrati a schemi di cifratura simmetrica, come AES);
- ricerca su dati cifrati, realizzata secondo uno schema di Searchable Encryption;
- trasferimento dati, realizzato con protocolli standard.

2.2 Ciphertext-Policy Attribute-Based Encryption

Per schemi di cifratura basata sugli attributi di tipo ciphertext-policy (Attribute-Based Encryption Schemes, in breve schemi CP-ABE), si intende un insieme di schemi di cifratura con le seguenti caratteristiche:

- ad ogni utente del sistema è fornita una Chiave Pubblica ABE (comune a tutti gli utenti) necessaria per eseguire le operazioni di cifratura;
- ad ogni utente viene associato un insieme di attributi che ne descrivono le caratteristiche;
- ad ogni utente viene assegnata una Chiave Segreta di Decifratura ABE che ne incorpora (intrinsecamente ed in maniera crittografica) gli attributi;
- ogni messaggio cifrato incorpora (intrinsecamente ed in maniera crittografica) una *policy* sugli attributi, che può essere o meno soddisfatta dagli attributi di un utente. La policy è stabilita *run time* dal mittente del messaggio e il messaggio è decifrabile esclusivamente (tramite la chiave segreta) dagli utenti i cui attributi (incorporati nella chiave) soddisfano la policy;
- la generazione di tutte le chiave e l'associazione di un utente con un insieme di attributi sono compiti di un entità *trusted* detta Authority . L'Authority inoltre possiede una Chiave Master ABE segreta da cui può derivare tutte le altre chiavi, incluse quelle degli utenti.

2.3 Entità definite

Le entità definite nel Dimostratore sono le seguenti:

- Authority
- Utenti
- Server di Ricerca
- Server di Archiviazione

2.3.1 Authority

L'Authority è un utente speciale del programma dotato di funzionalità che gli permettono di preparare il sistema all'utilizzo, di creare e rimuovere utenti, generare e revocare le chiavi di cifratura e decifratura, tramite la loro rigenerazione (2.4.1.1).
L'Authority in sé non è un utente come gli altri, ma può decidere di creare un utente personalizzato con il quale effettuare le operazioni permesse agli altri utenti.
Le funzionalità dell'Authority sono descritte nella Sezione 2.4.1.

2.3.2 Utente

L'entità Utente è dotata di uno username ed una password che gli permettono di accedere al programma.
Le funzionalità di un utente sono descritte nella Sezione 2.4.2.

2.3.3 Server di Archiviazione

Il Server di Archiviazione offre un'area di storage comune a tutti gli utenti tramite cui vengono scambiati i dati cifrati. Dal punto di vista implementativo può essere un'area condivisa su un servizio di Cloud. Non è un'entità *trusted*. Le funzionalità del Server di Archiviazione sono descritte nella Sezione 2.4.3.

2.3.4 Server di Ricerca

Il Server di Ricerca offre un semplice servizio di database con elementari query di ricerca. Non è un'entità *trusted*. Le funzionalità del Server di Ricerca sono descritte nella Sezione 2.4.4.

2.4 Funzionalità di ciascuna entità

2.4.1 Authority

L'Authority possiede un server che accede ad un database contenente i seguenti dati

- nomi degli utenti;
- password degli utenti (si veda 2.3.2);
- elenco di attributi associati a ciascun utente.

L'Authority svolge le seguenti funzioni:

- *Setup del sistema*
- *Creazione di un nuovo utente*
- *Rimozione di un utente*

2.4.1.1 Setup del sistema

Durante questa fase, dati un livello di sicurezza ed una curva ellittica ad esso corrispondente (la curva è un parametro chiave della definizione di uno schema 'ABE, si veda 6.3), l'Authority genera una Chiave Master ABE , mantenuta segreta, ed una Chiave Pubblica ABE , che viene invece distribuita a tutti gli utenti. Il Setup del sistema viene eseguito una prima volta alla prima installazione e nuovamente quando si presenta la necessità di cambiare i parametri di sicurezza.

2.4.1.2 Creazione di un utente

Durante questa fase l'Authority definisce un nuovo utente tramite uno *username* ed una *password*. Genera una Chiave Utente Segreta di Decifratura e la fornisce all'utente creato.

2.4.1.3 Rimozione di un utente

Durante questa fase l'Authority rimuove un utente dal sistema, cancellando i dati dello stesso dal proprio database.

2.4.2 Utenti

Un utente può svolgere le seguenti funzioni

- *Cifratura* di un file locale[2];
- *Decifratura* di un file locale;
- *Caricamento* di un file locale sul Server di Archiviazione ;
- *Ricerca* tramite parole chiave cifrate tra i file nel Server di Archiviazione ;
- *Scaricamento* in locale di un file sul Server di Archiviazione .

Ogni utente ha a disposizione i seguenti parametri privati

- Una Chiave Segreta di decifratura
- Una Chiave Segreta di ricerca

ed i seguenti parametri pubblici

- Una Chiave Pubblica (si veda 2.4.1.1);
- Il Tempo del sistema (un contatore che viene incrementato ad ogni nuova generazione di Chiave Pubblica da parte dell'Authority (si veda 6.4)).

Ha inoltre a disposizione una propria area di memoria in cui memorizzare i file in chiaro ed un'altra per i file cifrati.

[2] Per file *locale* si intende memorizzato nell'area privata dell'utente. La cifratura di un file locale genera un altro file locale (idem per la decifratura). Un file locale (cifrato) può essere caricato sul Server di Archiviazione oppure essere da questo scaricato per venire poi decifrato.

2.4.2.1 Cifratura

Tramite la Chiave Pubblica, ogni utente è in grado di cifrare un messaggio a cui deve associare una policy ammissibile. Notiamo che quindi, in linea di principio, anche un utente senza Chiave Segreta di Decifratura è in grado di cifrare in quanto la Chiave di Cifratura è pubblica.

2.4.2.2 Decifratura

Ogni utente in possesso di una Chiave Segreta di decifratura è in grado di decifrare solamente i testi cifrati la cui policy associata è soddisfatta dagli attributi della Chiave Segreta di decifratura.

2.4.2.3 Upload

Ogni utente può caricare file cifrati sul Server di Archiviazione. Inoltre ha la possibilità, al momento del caricamento, di associare al file cifrato un elenco cifrato di parole chiave, che verranno memorizzate solamente dal Server di Ricerca e in modo disaccoppiato con il Server di Archiviazione (l'accoppiamento può essere ristabilito solo dagli utenti attraverso il percorso di memorizzazione sul Server di Archiviazione, si veda 2.4.4).

2.4.2.4 Ricerca

Ogni utente in possesso di una Chiave Segreta di ricerca è in grado di effettuare ricerche cifrate tra i file nel Server di Archiviazione. La ricerca avviene inviando al Server di Ricerca una formula Booleana le cui foglie contengono possibili parole chiave cifrate (si noti che la struttura della formula non è cifrata). Il Server di Ricerca restituirà il percorso (sul Server di Archiviazione) e altri metedati dei file cifrati le cui parole chiave associate soddisfano tale formula (si veda 2.4.4).

2.4.2.5 Download

Ogni utente può scaricare i file cifrati che desidera dal Server di Archiviazione. Si noti che tuttavia non sarà in grado di decifrare i file la cui policy non è soddisfatta dagli attributi dell'utente stesso.

2.4.3 Server di Archiviazione

Il *Server di Archiviazione* serve per la memorizzazione remota dei file cifrati. Esso contiene esclusivamente i file cifrati nel formato definito nella Sezione 6.7.1. Il Server di Archiviazione non viene mai a conoscenza delle parole chiave cifrate associate a ciascun file.

2.4.4 Server di Ricerca

Il *Server di Ricerca* possiede un database in cui memorizza i metadati relativi a ciascun file che è stato caricato sul Server di Archiviazione .
I metadati associati a ciascun file cifrato sono i seguenti

- insieme di parole chiave cifrate per la ricerca (l'insieme può anche essere vuoto),
- policy associata,
- nome del file cifrato,
- percorso del file cifrato nel Server di Archiviazione ,
- nome del file utilizzato come chiave pubblica,
- nome del file utilizzato per il nome della curva ellittica (6.3),
- livello di sicurezza della cifratura,
- nome dell'utente che ha cifrato il file,
- data di upload con precisione al secondo,
- tempo del sistema in cui è stato cifrato il file.

I primi due (insieme di parole chiave e policy associata) sono selezionate dall'utente, le altre inserite in modo automatico.

3 Installazione

L'installazione del Dimostratore VPSS si divide in tre passi:

1. installazione del programma Client (Authority e Utenti),
2. installazione del server MySql (Server di Ricerca e Server dell'Authority),
3. installazione del server FTP (Server di Archiviazione).

L'installazione del Client fornisce un programma ad interfaccia grafica, che permette di loggarsi al sistema come Authority o come Utente standard. Ricordando le finalità puramente dimostrative del programma, per semplicità le aree di memoria destinate ad ogni utente (contenenti la chiave segreta ed i testi in chiaro) possono risiedere sullo stesso pc, anche se idealmente gli utenti dovrebbero lavorare su macchine fisicamente separate.
L'installazione del server MySql fornisce un programma che simula il Server dell'Authority e il Server di Ricerca. Nel primo viene creato un database contenente i dati relativi agli utenti (nome utente, password e attributi). Nel secondo viene creato un database contenente i metadati (cifratore, livello di sicurezza, chiave pubblica utilizzata, percorso del file, ecc.) di ogni file cifrato caricato sul Server di Archiviazione, incluso un insieme di parole chiave cifrate associate al testo cifrato.
L'installazione del server FTP fornisce il Server di Archiviazione dei file cifrati (cloud), senza le parole chiave cifrate associate.
Il Dimostratore VPSS si appoggia su diverse librerie scritte in linguaggio Python e C. Di seguito viene fornito un elenco delle principali librerie con una breve descrizione:

- CHARM [1]. Fornisce uno strumento per realizzare in maniera rapida prototipi crittografici. Implementata in linguaggio Python. `http://charm-crypto.com/`
- PBC. Libreria scritta in linguaggio C per lo sviluppo di schemi crittografici basati sui pairing. Costruita sulla libreria GMP. `https://crypto.stanford.edu/pbc/`
- OpenSSL. E' uno strumento opensource per la realizzazione di protocolli SSL ed altre primitive crittografiche. Implementata in linguaggio C. `https://www.openssl.org/`
- GMP. Libreria per l'aritmetica a precisione arbitraria, interi con segno, numeri razionali e numeri in virgola mobile. Implementata in linguaggio C. `https://gmplib.org/`

Alcune di queste librerie sono fornite solo per ambiente di sviluppo Linux. Tale ambiente può essere simulato su un sistema operativo Windows tramite il software MinGW.

3.1 Materiale fornito

3.2 Installazione in Windows 7

Le istruzioni che seguono sono state testate su una macchina a 64 bit con sistema operativo Windows 7 in lingua inglese.
NOTA IMPORTANTE: tutti i programmi installati devono essere per piattaforme a 32 bit.
Seguire le istruzioni di installazione nell'ordine in cui sono presentate.
Eseguire le istruzioni della Sezione 3.2.1 sulla macchina in cui si vuole avviare il Client (sia per simulazione Utenti, che per simulazione Authority).
Eseguire le istruzioni della Sezione 3.2.2 sulla macchina in cui si vuole installare il Server di Ricerca e sulla macchina in cui si vuole utilizzare il Client per la simulazione Authority (poiché anche essa possiede un database).
Eseguire le istruzioni della Sezione 3.2.3 sulla macchina in cui si vuole installare il Server di Archiviazione.

3.2.1 Installazione Client

Eseguire le istruzioni in questa sezione sulla macchina in cui si desidera utilizzare il Client per la simulazione Utenti e per la simulazione Authority.

3.2.1.1 MinGw

Per installare *MinGW*, scaricare la versione aggiornata del software, oppure seguire le seguenti istruzioni

1. Navigare nella cartella
   `VPSS\win_exe_32`
2. Cliccare sul file
   `mingw-get-setup.exe`
3. Scegliere le opzioni di default.
4. Aprire *MinGW Installation Manager*
5. Selezionare (tasto destro e "mark for installation") i seguenti pacchetti
   - `mingw-developer-toolkit`
   - `mingw32-base`
   - `mingw32-gcc-ada`
   - `mingw32-fortran`
   - `mingw32-gcc-g++`
   - `mingw32-gcc-objc`
   - `msys-base`

6. Dal menu `installation` scegliere in successione `apply changes -> apply`
7. Creare il file `fstab` nella cartella `C:\MinGW\msys\1.0\etc\` in modo che contenga la riga
   `C:\MinGW /mingw`
8. creare una scorciatoia sul desktop a
   `C:\MinGw\msys\1.0\msys.bat`

3.2.1.2 Installazione moduli Python

Il Dimostratore VPSS richiede l'installazione sia di Python che di Python3. Per installare i moduli Python/Python3 necessari seguire le seguenti istruzioni. Gli eseguibili si trovano nella cartella `VPSS\win_exe_32`.

1. Installare *Python*
   Utilizzare l'eseguibile `python-2.7.10.msi`
2. Installare *Python3*
   Utilizzare l'eseguibile `python-3.4.3.msi`
3. Nella cartella `C:\Python34` modificare il nome del file `python.exe` in `python3.exe`
4. Installare *wget*
   Utilizzare l'eseguibile `wget-1.11.4-1-setup.exe`
5. Aggiungere i seguenti percorsi alla variabile `Path`:
   `C:\MinGW\bin;`
   `C:\MinGW\msys\1.0\bin;`
   `C:\Python27;C:\Python27\Scripts;`
   `C:\Python34;C:\Python34\Scripts;`
   `C:\Program Files (x86)\GnuWin32\bin;`
   seguendo le seguenti istruzioni:
   a) cliccare il tasto destro sulla cartella `Computer`
   b) cliccare in successione
      `Properties -> Advanced System Settings -> Advanced -> Environment Variables`
   c) editare la variabile `Path` nel frame `System variables` aggiungendo, per esempio, `C:\Program Files (x86)\GnuWin32\bin` seguito da ";"
6. Installare *WxPython*
   Utilizzare l'eseguibile `wxPython3.0-win32-3.0.2.0-py27.exe`
7. Installare i seguenti moduli Python:
   - *MySQLdb*
     Aprire la cartella `VPSS\win_exe_32` e
     utilizzare l'eseguibile `MySQL-python-1.2.5.win32-py2.7.exe`
   - *pycrypto*
     Aprire la cartella `VPSS\win_exe_32` e
     utilizzare sia l'eseguibile `pycrypto-2.5.win32-py2.7.exe` che l'eseguibile `pycrypto-2.6.1.win32-py3.4.exe`

- *pyparsing*
  Digitare `easy_install pyparsing` dal prompt dei comandi.
- *sphinx*
  Digitare `pip install sphinx` dal prompt dei comandi.

3.2.1.3 Installazione dipendenze

Seguire le seguenti istruzioni per installare le librerie GMP, OpenSSL, PBC e CHARM.

1. Copiare la cartella `VPSS` nella cartella
   `C:\MinGW\msys\1.0\home\<nome_utente>`
2. Installare *Microsoft CryptoApi*
   Aprire la cartella `VPSS\win_exe_32` e utilizzare l'eseguibile `CSPTSTS10.EXE`
3. Lanciare il file `msys.bat` per aprire il terminale MinGW (cliccando la scorciatoia precedentemente creata sul desktop)
4. Dal ternimale MinGW, navigare nella cartella `VPSS\CP-ABE-LIB`, e decomprimere i file
   `gmp-6.0.0a.tar.bz2`
   `openssl-1.0.2d.tar.gz`
   `pbc-0.5.14.tar`
   `pycrypto-2.6.1.tar.gz`
   con i comandi
   ```
   tar -xvjf gmp-6.0.0a.tar.bz2
   tar -xvf pbc-0.5.14.tar
   tar -xzvf openssl-1.0.2d.tar.gz
   tar -xzvf pycrypto-2.6.1.tar.gz
   ```
5. Dal ternimale MinGW, installare le seguenti librerie seguendo i rispettivi comandi
   a) *GMP*
      i. Navigare nella cartella
         `VPSS\CP-ABE-LIB\gmp-6.0.0`
      ii. digitare i seguenti comandi
         ```
         bash configure -prefix=/mingw -disable-static -enable-shared
         make
         make install
         ```
   b) *OpenSSL*
      i. Navigare nella cartella
         `VPSS\CP-ABE-LIB\openssl-1.0.2d`
      ii. digitare i seguenti comandi
         ```
         ./config -openssldir=/mingw -shared
         make
         make install
         ```

c) *PBC*

i. Navigare nella cartella
`VPSS\CP-ABE-LIB\pbc-0.5.14`

ii. digitare i seguenti comandi
```
bash configure -prefix=/mingw -disable-static -enable-shared
make
make install
```

d) *CHARM*

i. Navigare nella cartella
`VPSS\charm-dev`

ii. digitare i seguenti comandi
```
bash configure.sh -prefix=/mingw -python=/c/Python34/python3.exe
make
make install
```

iii. Per poter generare curve personalizzate
Copiare (sovrascrivendo il file precedente con lo stesso nome) il file
`VPSS\demo_vpss\pairingcurves.py`
nella cartella
`C:\Python34\Lib\site-packages\Charm_Crypto-0.43-py3.4-win32.egg\charm\toolbox`

3.2.2 Installazione server MySql

Installare il software MySql Server sia nella macchina in cui verrà utilizzato il Client (per la simulazione Authority) sia nella macchina in cui verrà utilizzato il Server di Ricerca.
Se la macchina in cui viene installato il Server di Ricerca è diversa da quella in cui è stato installato il Client, allora prima di seguire le seguenti instruzioni installare Python seguendo le istruzioni della Sezione 3.2.1.2.
Per installare MySql seguire le seguenti istruzioni.

1. Installare *MICROSOFT .NET FRAMEWORK 4 FOR MICROSOFT WINDOWS OPERATING SYSTEM*
Utilizzando l'eseguibile
`dotNetFx40_Full_setup.exe`
nellca cartella `VPSS\win_exe_32` o scaricando l'eseguibile da
`go.microsoft.com/fwlink/?LinkId=181012`
2. Installare *MySql* utillizzando l'eseguibile
`mysql-installer-web-community-5.6.25.0.msi`
3. Durante l'installazione scegliere l'opzione `Full`
4. Alla richiesta `Check Requirements` non aggiungere nessuna opzione e cliccare `Execute`
5. Durante il setup di MySql settare la password `mysql123`

3.2.3 Installazione server FTP

Installare un server FTP nella macchina si vuole installare il Server di Archiviazione .
In questa sezione sono descritte le istruzioni per installare il software *FileZilla*.
Gli eseguibili a cui si fa riferimento sono contenuti nella cartella `VPSS\win_exe_32`.
Se la macchina in cui viene installato il Server di Archiviazione è diversa da quella in cui è stato installato il Client, allora prima di seguire le seguenti instruzioni installare Python seguendo le istruzioni della Sezione 3.2.1.2.

1. Installare *FileZilla Client* utilizzando l'eseguibile
   `FileZilla_3.13.1_win64-setup.exe`
2. Installare *FileZilla Server* utilizzando l'eseguibile
   `FileZilla_Server-0_9_53.exe`
3. Aprire Filezilla Server senza inserire una password.
4. Nel frame `Page -> General`
   cliccare su `Edit -> Users -> Add`
5. Aggiungere un utente con nome `cloud` e password `cloud`
6. Creare la cartella
   `C:\FTP`
7. Nel frame `Page -> Shared folders`
   a) aggiungere la cartella `C:\FTP` come *home directory*
   b) selezionare la cartella `C:\FTP`
   c) spuntare le caselle `read`, `write`, `delete`

3.3 Installazione in Ubuntu 14.04

Le istruzioni che seguono sono state testate su una macchina a 64 bit con sistema operativo Ubuntu 14.04 LTS, in lingua inglese.
Seguire le istruzioni di installazione nell'ordine in cui sono presentate.
Ci sono due possibili installazioni: la prima è più rapida ed automatizzata e consente di installare tutti i componenti su un'unica macchina (3.3.1), la seconda è più lenta ma permette di utilizzare macchine diverse e creare così un ambiente più vicino a quello di utilizzo ideale (3.3.2, 3.3.3, 3.3.4). In particolare:

- Eseguire le istruzioni della Sezione 3.3.1 per installare sia il Client (per simulazione Utenti e Authority) sia i Server di Archiviazione e Ricerca in un'unica macchina.
- Eseguire le istruzioni della Sezione 3.3.2 sulla macchina in cui si vuole avviare il Client (sia per simulazione Utenti, che per simulazione Authority).
- Eseguire le istruzioni della Sezione 3.3.3 sulla macchina in cui si vuole installare il Server di Ricerca e sulla macchina in cui si vuole utilizzare il Client per la simulazione Authority (poiché anche essa possiede un database).

- Eseguire le istruzioni della Sezione 3.3.4 sulla macchina in cui si vuole installare il Server di Archiviazione .

Assicurarsi di avere una connessione internet funzionante.

3.3.1 Installazione Veloce

Le seguenti istruzioni possono essere eseguite per installare su un'unica macchina il Client per utenti e authority ed i Server di Archiviazione e Ricerca.

1. Da terminale, navigare nella cartella
   `VPSS\demo_vpss`
2. Digitare
   `bash INSTALL_CLIENT.sh`
3. Quando viene richiesta la password MySql inserire
   `mysql123`
4. Digitare
   `bash INSTALL_SERVER.sh`
5. Quando viene richiesta la password FTP inserire
   `cloud`

3.3.2 Installazione Client

Eseguire le istruzioni in questa sezione sulla macchina in cui si desidera utilizzare il Client per la simulazione Utenti e per la simulazione Authority .
Da terminale, digitare i seguenti comandi

1. Settare i permessi della cartella `VPSS`
   ```
   sudo chmod -R 755 VPSS
   ```
2. Installare Client *FTP* e *MySql*
   ```
   sudo apt-get install -yes ftp
   sudo apt-get install -yes mysql-client
   sudo apt-get install -yes mysql-server
   ```
3. Installare moduli *Python*
   ```
   sudo apt-get install -yes python
   sudo apt-get install -yes python-mysqldb
   sudo apt-get install -yes python3
   sudo apt-get install -yes python-wxgtk2.8
   ```
4. Installare il programma *M4*
   ```
   sudo apt-get install -yes m4
   ```

5. Installare la libreria *GMP*
   ```
   cd ../CP-ABE-LIB/gmp-6.0.0
   ./configure
   make
   sudo make install
   ```
6. Installare il programma *FLEX* e *BISON*
   ```
   sudo apt-get install -yes flex sudo apt-get install -yes bison
   ```
7. Installare il programma *OPENSSL*
   ```
   sudo apt-get install -yes libssl-dev
   ```
8. Installare la libreria *PBC*
   ```
   cd ../CP-ABE-LIB/pbc-0.5.14
   ./configure
   make
   sudo make install
   ```
9. Installare la libreria *CHARM*
   ```
   cd ../../charm-0.43
   sh configure.sh
   sudo make
   sudo make install
   ldconfig
   ```

3.3.3 Installazione server MySql

Installare il software MySql Server sia nella macchina in cui verrà utilizzato il Client (per la simulazione Authority) sia nella macchina in cui verrà utilizzato il Server di Ricerca .
Se la macchina in cui viene installato il Server di Ricerca è diversa da quella in cui è stato installato il Client, allora prima di seguire le seguenti instruzioni installare Python digitando i comandi `sudo apt-get install -yes python`
`sudo apt-get install -yes python-mysqldb`

Per installare MySql seguire le seguenti istruzioni.

1.
2. Installare Server*MySql*
   ```
   sudo apt-get install -yes mysql-server
   ```
3. Configurare il server MySql, assicurandosi che il file `/etc/mysql/mysql.conf.d/mysqld.cnf` contenga le seguenti righe (l'ultima commentata)
   ```
   [mysqld]
   user            = mysql
   pid-file        = /var/run/mysqld/mysqld.pid
   ```

```
socket          = /var/run/mysqld/mysqld.sock
port            = 3306
basedir         = /usr
datadir         = /var/lib/mysql
tmpdir          = /tmp
language        = /usr/share/mysql/English
bind-address    = <HOST_IP_ADDRESS>
# skip-networking
```

Dovrebbe essere sufficiente digitare i comandi

```
IP="$(ifconfig | grep -A 1 'eth0' | tail -1 | cut -d ':' -f 2 | cut -d ' ' -f 1)"
sudo sed -i "s/bind-address/bind-address = "$IP"\n#/g" /etc/mysql/my.cnf
```

4. Relanciare MySql con il comando
   `sudo service mysql restart`

3.3.4 Installazione server FTP

Installare un server FTP nella macchina si vuole installare il Server di Archiviazione.
In questa sezione sono descritte le istruzioni per installare il software *FileZilla*.
Gli eseguibili a cui si fa riferimento sono contenuti nella cartella `VPSS\win_exe_32`.
Se la macchina in cui viene installato il Server di Archiviazione è diversa da quella in cui è stato installato il Client, allora prima di seguire le seguenti instruzioni installare Python digitando i comandi `sudo apt-get install -yes python`

```
sudo apt-get install -yes python-mysqldb
```

Per installare il server FTP seguire digitare il comando
`sudo apt-get install -yes ftp`
Configurare il server FTP eseguendo le seguenti istruzioni

1. Assicurarsi che il file `/etc/vsftpd.conf` contenga le righe seguenti
   ```
   local_enable=YES
   write_enable=YES
   userlist_enable=YES
   userlist_deny=NO
   userlist_file=/etc/vsftpd.user_list
   ```
   Dovrebbe essere sufficiente digitare i seguenti comandi

   ```
   sudo sed -i "s/local_enable=NO/local_enable=YES/g" /etc/vsftpd.conf
   sudo sed -i "s/#write_enable/write_enable/g" /etc/vsftpd.conf
   sudo sed -i "s/write_enable=NO/write_enable=YES/g" /etc/vsftpd.conf

   sudo sed -i "/userlist_enable=YES/d" /etc/vsftpd.conf
   sudo sed -i "/userlist_deny=NO/d" /etc/vsftpd.conf
   sudo sed -i "/userlist_file=\/etc\/vsftpd.user_list/d" /etc/vsftpd.conf
   ```

```
echo "userlist_enable=YES" | sudo tee -a /etc/vsftpd.conf
echo "userlist_deny=NO" | sudo tee -a /etc/vsftpd.conf
echo "userlist_file=/etc/vsftpd.user_list" | sudo tee -a /etc/vsftpd.conf
```

2. Creare il file
   `/etc/vsftpd.user_list`
   e, per aggiungere l'utente `cloud`, aggiungere la riga
   `cloud`
   Per farlo è possibile utilizzare i comandi

```
if [ -f /etc/vsftpd.user_list ]; then
    sudo sed -i "/cloud/d" /etc/vsftpd.user_list
fi
echo "cloud" | sudo tee -a /etc/vsftpd.user_list
```

3. Editare `/etc/shells` aggiungendo la riga
   `/bin/false`
   Per farlo utilizzare il comando

```
sudo sed -i "\/bin\/false/d" /etc/shells
echo "/bin/false" | sudo tee -a /etc/shells
```

4. Aggiungere il nuovo utente `cloud` con password `cloud` utilizzando i seguenti comandi

```
FTP_CLOUD_FOLDER="/home/cloud"
sudo mkdir -p ${FTP_CLOUD_FOLDER}
sudo useradd cloud -d ${FTP_CLOUD_FOLDER} -s /bin/false
sudo passwd "cloud"
sudo chown -R cloud:users ${FTP_CLOUD_FOLDER}
```

5. Relanciare il demone con il comando
   `sudo service vsftpd restart`

4 Setup del sistema

Assicurarsi di avere copiato la cartella `VPSS` sulle macchine in cui sono stati installati [1]

- il Client
- il Server di Ricerca
- il Server di Archiviazione

La configurazione del Dimostratore è contenuta in sei file memorizzati nella cartella `VPSS\demo_vpss`, tre dedicati all'impostazione statica (generale) del sistema (Sezione 4.1) e tre relativi invece alla sua configurazione dinamica (Sezione 4.2).

4.1 File di configurazione statici

Dei tre file descritti in questa sezione, uno riguarda la configurazione di rete dei server (sezione 4.1.1) e due i parametri statici dell'ABE (4.1.2 e 4.1.3). Anche se ai fini dimostrativi del progamma in linea di massima non c'è motivo di farlo, è possibile modificare manualmente il contenuto di questi file, prestando però molta attenzione al loro significato e formato perché l'inserimento di dati errati impedirrebbe il corretto funzionamento del sistema.

4.1.1 Il file *def_servers.txt*

In questo file sono contenuti gli indirizzi IP, lo username e la password del Server dell'Authority, del Server di Ricerca e del Server di Archiviazione. Inoltre per il Server dell'Authority e per il Server di Ricerca sono contenuti il nome del database di ciascun server e la password dell'utente root del server MySql.
Un esempio di contenuto del file è il seguente

```
AUTHORITY_SERVER=localhost
AUTHORITY_USERNAME=auth
AUTHORITY_PASSWORD=auth123
AUTHORITY_DB_NAME=authdb
AUTHORITY_ROOT=root
AUTHORITY_ROOT_PASSWORD=mysql123
```

[1] Dato lo scopo dimostrativo del programma, è immaginabile che per semplicità le tre macchine possano coincidere.

```
SEARCH_SERVER=localhost
SEARCH_USERNAME=searchuser
SEARCH_PASSWORD=search123
SEARCH_NAME=searchdb
SEARCH_ROOT=root
SEARCH_ROOT_PASSWORD=mysql123
CLOUD_SERVER=localhost
CLOUD_USERNAME=cloud
CLOUD_PASSWORD=cloud
```

I parametri più importanti di questo file sono gli indirizzi IP dei tre server, in particolare ciò che è scritto a destra del carattere "=" ("uguale") nelle righe

- `AUTHORITY_SERVER`
- `SEARCH_SERVER`
- `CLOUD_SERVER`

In questo campo è possibile inserire l'indizzo IP del server di riferimento, ad esempio `127.0.0.1`, oppure la parola chiave "`localhost`" (senza le virgolette).
Si consiglia di non modificare gli altri campi in modo da rimanere allineati con le istruzioni di installazione riportate nella Sezione 3.

4.1.2 Il file *choose_abe_scheme.py*

In questo file è possibile selezionare lo schema ABE utilizzato per le operazione di generazione delle chiavi, di cifratura e decifratura. Il contenuto di default del file è il seguente

```
"""
uncomment the file you wish to import
each file defines a different abe scheme
"""
from abenc_waters09 import *
#from abenc_bsw07 import *
```

Lasciare senza commento solo la riga rappresentante lo schema che si vuole utilizzare. Per commentare le altre righe aggiungere il carattere "#" all'inizio della riga.
Attualmente gli schemi selezionabili sono due:

1. Lo schema descritto in [4]
2. Lo schema descritto in [2]

Il primo dei due schemi è più efficiente e quindi viene proposto di default. Dal punto di vista dimostrativo delle funzionalità dell'ABE la scelta dello schema è poco rilevante, ma è permessa per evidenziare l'elasticità dell'architettura implementata.

4.1.3 Il file *pairingcurves.py*

In questo file è possibile inserire il dominio dei parametri di curve ellittiche personalizzate.
Istruzioni su come generare curve ellittiche personalizzate con la libreria *PBC* sono contenute all'interno del file.
Al link (*https://crypto.stanford.edu/pbc/manual/ch08s03.html*) si trova un documento che tratta il significato dei parametri delle curve inserite nel file. Tale descrizione esula dagli scopi di questa documentazione.
La descrizione del file è stata qui riportata per completezza, ma al fine di dimostrare le funzionalità dell'architettura implementata non vi è in effetti ragione di modificarne il contenuto.

4.2 File di configurazione dinamici

I tre file descritti in questa sezione sono dedicati alla definizione degli utenti (4.2.2) e dei parametri dinamici dell'ABE, cioè l'insieme degli attributi (4.2.1) e le policy su di essi definiti (4.2.3).
Come descritto più avanti, il programma Client permette di modificare il contenuto dei file relativi agli utenti e alle policy, mentre quello degli attributi deve essere correttamente configurato manualmente. In ogni caso nella sezione 4.3 è descritta la procedura automatica per ripristinare il contenuto di default di tutti e tre i file (costituito da un insieme minimo di valori che permettono l'utilizzo immediato del Dimostratore).

4.2.1 Il file *def_attributes.txt*

Questo file contiene l'elenco, detto *universo*, dei possibili attributi del sistema. Il formato del file prevede che l'elenco sia scritto su un'unica riga, separando gli attributi con il carattere "," ("virgola"). Gli attributi devono contenere caratteri alfanumerici, ed il primo carattere deve essere alfabetico. I caratteri alfabetici devono essere maiuscoli. In 4.3.2 è descritto come riportare il file al contenuto iniziale.
Un file d'esempio può essere il seguente

```
ATTR1,ATTR2,ATTR3,ATTR4,ATTR5
```

4.2.2 Il file *def_users.txt*

In questo file è contenuto l'elenco degli utenti iniziali del sistema (successivamente al primo avvio, gli utenti possono essere aggiunti e rimossi dal client Authority), con la rispettiva password di accesso e l'elenco degli attributi ad essi associati. In 4.3.2 è descritto come riportare il file al contenuto iniziale.
Un esempio di contenuto del file è il seguente

```
utente1:123:ATTR1
utente2:123:ATTR1,ATTR2
utente3:123:ATTR1,ATTR2,ATTR3,ATTR4
AUTHORITY:123:ATTR1,ATTR2,ATTR3,ATTR4,ATTR5
```

Ogni riga rappresenta i dati relativi ad un utente. I dati di ciascun utente sono raggruppabili in 3 campi separati dal carattere ":" ("due punti").
Il primo campo contiene il nome dell'utente, il secondo campo la password di accesso dell'utente. Questi due campi devono contenere esclusivamente caratteri alfanumerici.
Il terzo campo rappresenta l'elenco degli attributi relativi all'utente. Gli attributi sono separati dal carattere "," e devono essere scelti tra l'elenco di attributi definiti nel file `def_attributes.txt`.

4.2.3 Il file *def_policies.txt*

Questo file contiene le possibili policy con cui cifrare i file in chiaro. Costituito inizialmente da un insieme di policy pre-costituite (in 4.3.2 è descritto come riportare il file al contenuto iniziale), questo file viene integrato dalle nuove policy costruite anche nel corso dell'esecuzione del Dimostratore (si veda Sezione 5.4.1.1).
Un esempio di contenuto del file è il seguente

```
ATTR1
ATTR2
ATTR3
ATTR4
ATTR5
ATTR1 and ATTR2
ATTR1 and ATTR3
ATTR1 and ATTR4
ATTR1 and ATTR5
ATTR1 or ATTR2
ATTR1 or ATTR3
ATTR1 or ATTR4
ATTR4 or (ATTR1 and ATTR2)
ATTR5 or (ATTR1 and ATTR2) or (ATTR4 or (ATTR1 and ATTR2))
```

Ogni riga contiene una policy. Ciascuna policy deve essere una formula Booleana in forma disgiuntiva, senza la presenza dell'operatore di negazione. Le foglie di ciascuna formula devono essere attributi scelti dall'elenco del file `def_attributes.txt`.

4.3 Reset configurazioni

4.3.1 Reset delle macchine

Durante l'utilizzo del Dimostratore, lo stato del Client, del Server di Ricerca e del Server di Archiviazione vengono ovviamente modificati. Le seguenti istruzioni possono essere eseguite ogni qualvolta si desideri riportarli allo stato iniziale (reset). Sebbene sia possibile eseguire il reset di ciascuna macchina singolarmente, quando si effettua il reset di una macchina è consigliabile eseguire anche il reset delle altre due macchine, in modo da mantenerne lo stato allineato e coerente. Per la stessa ragione è inoltre preferibile eseguire nella stessa occasione il reset dei file di configurazione dinamici, come descritto in 4.3.2.

1. Sulla macchina in cui è installato il Server di Ricerca
   a) Dal prompt dei comandi navigare nella cartella
      `VPSS\demo_vpss`
   b) Digitare il comando
      `python SET_SEARCH_server.py`
2. Sulla macchina in cui è installato il Server di Archiviazione
   a) Dal prompt dei comandi navigare nella cartella
      `VPSS\demo_vpss`
   b) Digitare il comando
      `python SET_CLOUD_server.py`
3. Sulla macchina in cui è installato il Client
   a) Dal prompt dei comandi navigare nella cartella
      `VPSS\demo_vpss`
   b) digitare i comandi
      `python SET_ABE_client.py`
      `python SET_AUTHORITY_server.py`

4.3.2 Reset dei file di configurazione dinamici

Ogni qualvolta si desideri resettare lo stato iniziale dei file di configurazione

- def_attributes.txt (si veda 4.2.1);
- def_users.txt (si veda 4.2.2);
- def_policies.txt (si veda 4.2.3);

eseguire le seguenti istruzioni sulla macchina in cui è installato il client:

1. Dal prompt dei comandi navigare nella cartella
   `VPSS\demo_vpss`
2. Digitare il comando
   `python SET_FILES.py`

Con la procedura descritta il contenuto dei tre file viene riportato al loro valore pre-impostato, che definisce una configurazione minima comunque utile a testare le funzionalità del sistema.
Quando si esegue il reset dei file di configurazione è consigliabile eseguire anche il reset delle macchine, come descritto in 4.3.1.

5 Utilizzo del Dimostratore

Completata l'installazione del Dimostratore come descritto nel Capitolo 3, tutte le operazioni, incluse le interazioni con il Server di Archiviazione e il Server di Ricerca, vengono eseguite attraverso il Client, il quale simula l'attività sia dell'Authority sia degli utenti.
Prima di avviare il Client del Dimostratore per la prima volta, assicurarsi di

1. aver installato correttamente il Server dell'Authority, il Server di Ricerca, il Server di Archiviazione, come spiegato nella Sezione 3;
2. aver copiato sulla propria macchina la cartella `VPSS`;
3. aver settato le configurazioni allo stato iniziale, seguendo le istruzioni della Sezione 4.3 (o avendole eventualmente modificate secondo quanto descritto nella Sezione 4, in particolare con riferimento all'universo degli attributi (4.2.1)).

5.1 Avvio del programma

Per avviare il Client

1. Tramite prompt dei comandi navigare nella cartella
   `VPSS\demo_vpss`
2. Digitare il comando
   `python vpss.py`

5.2 Finestra *Login*

Dopo aver avviato il Client, compare una finestra di login divisa in due pannelli, uno relativo al login degli Utenti, uno relativo al login dell'Authority.
Al primo avvio del programma il pulsante `Login come UTENTE` è disabilitato, poiché l'Authority deve ancora generare e distribuire le chiavi al sistema. Questo accade anche dopo un reset (4.3.1, 4.3.2)[1].
Se il contenuto dei campi `Nome Utente` e `Password` nel pannello relativo agli utenti sono corretti, cliccando sul pulsante `Login come UTENTE` la finestra Login si chiude e compare la finestra Utente.
Se il contenuto del campo `Password` nel pannello relativo all'Authority è corretto, cliccando sul pulsante `Login come AUTHORITY` la finestra Login si chiude e compare la finestra Authority.
Il controllo di correttezza username/password viene effettuato interrogando un database presente sul Server dell'Authority, caricato inizialmente secondo i dati contenuti nel file def_users.txt.

[1] Dopo un reset alcuni utenti sono presenti, in quanto ne viene ripristinato l'elenco predefinito, ma è comunque necessario fare il login come Authority per assegnare loro le chiavi.

5.3 Finestra *Authority*

La finestra relativa all'Authority presenta due tab:

1. il tab Setup,
2. il tab Gestione utenti.

Tramite questi due tab è possibile generare le chiavi del sistema, distribuirle, e creare e rimuovere utenti. Per uscire dalla finestra relativa all'Authority e tornare alla finestra Login, cliccare il pulsante `Logout`.

5.3.1 Tab *Setup*

Il tab *Setup* permette di generare la *Chiave Master* custodita dall'Authority e la *Chiave Pubblica*, custodita in un'area comune a tutti gli utenti. Le due chiavi sono matematicamente collegate e la Chiave Pubblica è generata a partire dalla Chiave Master. Entrambe le chiavi sono generate una volta definito il livello di sicurezza del crittosistema e la curva ellittica su cui eseguire le diverse operazioni relative al protocollo ABE. E' necessario generare le due chiavi almeno una volta dopo il reset del sistema.
Per generare una Chiave Master ed una Chiave Pubblica seguire le seguenti istruzioni:

1. Dal menù a tendina a fianco del campo `Selezionare livello di sicurezza:` selezionare il livello di sicurezza e la relativa curva
2. Cliccare sul pulsante `Genera`
3. Nella finestra che compare cliccare il pulsante `Yes`. Cliccando il pulsante `No` o il pulsante `Cancel` la generazione viene interrotta.
4. Se la generazione è avvenuta correttamente, una finestra informa l'utente del percorso in cui sono state salvate la Chiave Master e la Chiave Pubblica, rispettivamente nei file `master.k` e `public.k`. Cliccare il pulsante `OK`.
5. A questo punto l'Authority esegue in automatico le seguenti operazioni, che potrebbero richiedere qualche minuto:
   a) Ogni file presente sul Server di Archiviazione viene scaricato in locale, decifrato e ricifrato con la nuova chiave pubblica.
   b) Per ogni utente del sistema, a partire dalla nuova Chiave Master, viene generata una Chiave Segreta di decifratura contenente intrinsecamente gli attributi relativi all'utente.
   c) La chiave viene distribuita a ciascun utente (salvata nella sua area di memoria).
   d) Il tempo del sistema, contenuto nel file pubblico `time.t`, viene incrementato di un'unità.

   Se le suddette operazioni sono avvenute con successo una nuova finestra compare per informare l'utente della riuscita delle operazioni. Cliccare il pulsante `OK`.

Maggiori dettagli

La Chiave Master viene salvata nel file
`master.k`
contenuto nella cartella
`VPSS\demo_vpss\authority\master_keys`
visibile solo all'Authority.

La Chiave Pubblica viene salvata nel file
`public.k`
contenuto nella cartella
`VPSS\demo_vpss\public_parameters`
visibile a tutti gli utenti.

La Chiave Segreta dell'utente `username` viene salvata nel file
`username_secret.k` contenuto nella cartella
`VPSS\demo_vpss\users\username\secret_keys\ABE_sk`
visibile solo all'utente `username`.

Il file
`time.t`
è contenuto nella cartella
`VPSS\demo_vpss\public_parameters`
visibile a tutti gli utenti.

5.3.2 Tab *Gestione utenti*

Il tab *Gestione utenti* permette all'Authority di generare un nuovo utente del sistema o di rimuovere un utente esistente.

5.3.2.1 Creazione nuovo utente

Per creare un nuovo utente del sistema seguire le seguenti istruzioni

1. Nel campo `Nome utente:` inserire il nome che si desidera attribuire al nuovo utente. Il nome deve contenere esclusivamente caratteri alfanumerici.
2. Il campo `Password:` è settato di default al valore `123` e per semplicità non può essere cambiato (sarebbe infatti irrilevante ai fini dimostrativi del software).
3. Cliccare sul pulsante `Crea Utente`. Se il nome utente inserito è già esistente o contiene caratteri non alfanumerici, compare un messaggio di errore e la generazione viene interrotta. Altrimenti compare una finestra in cui selezionare gli attributi dell'utente, scegliendo dall'insieme di attributi definito nel file `def_attributes.txt`
    - Se viene cliccato il pulsante `Cancel` la creazione dell'utente viene interrotta.

- Se non viene selezionato nessun attributo e viene cliccato il pulsante `OK` viene creato un utente non abilitato né alla decifratura né alla ricerca tra i file cifrati, ovvero tale utente non è in possesso di una Chiave Segreta di decifratura né di una Chiave Segreta di ricerca.
- Se viene selezionato almeno un attributo e viene cliccato il pulsante `OK` viene creato un nuovo utente al quale viene assegnata una Chiave Segreta di decifratura, generata sul momento a partire dalla Chiave Master corrente e contenente gli attributi selezionati, ed una Chiave Segreta di Ricerca, uguale per tutti gli utenti.

4. Se l'utente è stato creato correttamente compare un messaggio di conferma creazione utente. Cliccare il pulsante `OK`.
   Inoltre il database dell'Authority viene aggiornato con l'inserimento del nuovo utente ed i rispettivi attributi associati.

Maggiori dettagli

La creazione di un utente con nome `username` implica la creazione di una nuova cartella `username` all'interno della cartella `VPSS\users`. Successivamente alla creazione dell'utente `username` la cartella `VPSS\users\username`
sarà così composta

- `\ciphertext` cartella contenente i file cifrati dell'utente
- `\plaintext` cartella contenente i file in chiaro dell'utente
- `\secret_keys` cartella contenente le chiavi segrete dell'utente
  - `\ABE_sk` cartella contenente la chiave segreta ABE dell'utente
    - `username_secret.k` file contenente la chiave segreta ABE (si veda 5.4.1.2)
  - `\AES_sk` cartella contenente la chiave simmetrica segreta AES dell'utente
  - `\SEARCH_sk` cartella contenente la chiave segreta di ricerca dell'utente
    - `search.k` file contenente la chiave segreta di ricerca

5.3.2.2 Rimozione utente

Per rimuovere un utente dal sistema seguire le seguenti istruzioni

1. Selezionare un utente dal menù a tendina sopra il pulsante `Rimuovi Utente`
2. Cliccare il pulsante `Rimuovi Utente`.

Non è possibile rimuovere l'utente `AUTHORITY`.

Maggiori dettagli

Quando un utente con nome `username` viene rimosso, vengono rimossi i seguenti oggeti dal sistema

- l'intera cartella relativa all'utente,
- i dati relativi all'utente presenti nel database dell'Authority.

5.4 Finestra *Utente*

La finestra relativa all'Utente presenta quattro tab:

1. il tab Cifra, che permette di cifrare localmente i file in chiaro dell'utente;
2. il tab Decifra, che permette di decifrare localmente i file cifrati dell'utente;
3. il tab Trasferimento file, che permette di caricare file in chiaro sul Server di Archiviazione; di effettuare ricerche per parole chiave sul Server di Archiviazione; di scaricare file cifrati dal Server di Archiviazione;
4. il tab Visualizza contenuto cartelle, che permette di visualizzare il contenuto delle cartelle e dei file relativi all'utente.

Nella parte alta della finestra vengono visualizzati il nome dell'utente loggato e l'insieme di attributi ad esso associati.
Per uscire dalla finestra relativa all'Utente e tornare alla finestra Login, cliccare il pulsante `Logout`.
Per il resto della sezione corrente indicheremo con `username` il nome dell'utente loggato al sistema.
Come si può osservare, le operazioni di cifra/decifra (in locale) e quelle di ricerca e di caricamento/scaricamento (sul Server di Archiviazione) sono mantenute distinte per rendere chiaro il funzionamento del sistema.

5.4.1 Tab *Cifra*

Il tab *Cifra* permette di cifrare, utilizzando la Chiave Pubblica, i file in chiaro contenuti nella cartella
`VPSS\users\username\plaintexts`
associando al relativo file cifrato, in maniera intrinseca, una policy di cifratura, creata o scelta dall'utente al momento della cifratura. I file cifrati in questo modo saranno decifrabili solamente dagli utenti che possiedono una Chiave Segreta di decifratura contenente un insieme di attributi che soddisfi la suddetta policy.

5.4.1.1 Creazione di una policy

Un elenco di possibili policy è contenuto nel file `def_policies.txt`. Oltre a queste policy è possibile creare delle policy personalizzate.
Per creare una policy seguire le seguenti istruzioni

1. Cliccare il pulsante `Crea` a fianco del label `Crea una policy:`

2. Nella finestra `Crea Policy` che compare, cliccare il pulsante `and` o il pulsante `or`
3. Selezionare almeno due elementi tra quelli dell'elenco proposto nella nuova finestra che compare
4. Cliccare il pulsante `OK`
5. La policy creata viene ora visualizzata in un label nella finestra `Crea Policy`. Se la policy visualizzata è corretta cliccare il pulsante `Aggiungi all'elenco` per aggiungere la policy al file `def_policies.txt`
6. Seguire i precedenti passi fino a che non viene creata la policy desiderata
7. Cliccare sul pulsante `Fine`

A questo punto le policy create seguendo i passi precedenti saranno presenti nel menù a tendina sotto il pulsante `Crea`.

5.4.1.2 Cifratura file

Per cifrare un messaggio rispetto ad una policy seguire le seguenti istruzioni

1. Cliccare sul pulsante `File...` per scegliere un file dalla cartella `VPSS\users\username\plaintexts`
2. Selezionare uno dei file presenti e cliccare il pulsante `Open`
3. Selezionare una policy dal menù a tendina sotto il pulsante `Crea`
4. Se la policy desiderata non è presente nel menù, crearne una personalizzata seguendo le istruzioni della Sezione 5.4.1.1
5. Cliccare il pulsante `Cifra`
6. Cliccare il pulsante `OK` nella finestra informativa che viene visualizzata

Il nome del file cifrato è sempre costuito aggiungendo l'estensione `pdf` al nome del file in chiaro (ad esempio il file in chiaro `prova.pdf` genera il file cifrato `prova.pdf.enc`). Il file cifrato viene posto nella cartella `VPSS\users\username\ciphertexts`. Se nella cartella di destinazione è già presente un file con lo stesso nome, viene aggiunto in coda al nome del file senza estensione il primo indice incrementale libero maggiore o uguale a 2, ad esempio `prova2.pdf.enc`.

Maggiori dettagli

Durante la cifratura del file `prova.pdf` avvengono le seguenti operazioni

1. Viene creata una stringa di *metadati* contenente le seguenti informazioni:
   - il *tempo* del sistema, che rappresenta il numero progressivo assegnato ad ogni nuova Chiave Pubblica;
   - il nome dell'utente che cifra il file
   - il livello di sicurezza della cifratura
   - il percorso del file che definisce la curva ellittica utilizzata per il protocollo ABE

- il percorso del file contenente Chiave Pubblica utilizzata
- la policy utilizzata

2. Viene creata randomicamente una password segreta `password.k` temporanemente memorizzata nella cartella
   `VPSS\users\username\secret_keys\AES_sk`
3. Il file `password.k` viene cifrato con la Chiave Pubblica ABE `public.k` nel file `password.k.enc` contenuto temporaneamente nella cartella
   `VPSS\users\username\ciphertexts`
4. Utilizzando il contenuto del file `password.k` come password ed il generatore random del sistema operativo, vengono generati *salt*, *IV* e *chiave simmetrica* secondo la funzione di derivazione della chiave PBKDF2 (Password-Based Key Derivation Function 2, `https://tools.ietf.org/html/rfc2898`, [3]).
5. Il salt, l'IV e la chiave simmetrica generati vengono utilizzati per cifrare il file in chiaro `prova.pdf` con la cifrante AES-128 in modalità CBC.
6. Nella cartella
   `VPSS\users\username\ciphertexts`
   viene creato il file cifrato `prova.pdf.enc` contenente la concatenazione di metadati, contenuto del file `password.k.enc` e cifratura di `prova.pdf` (contenente anche salt e IV), come descritto nella Sezione 6.7.1.
7. Il file `password.k` viene eliminato

5.4.2 Tab *Decifra*

Il tab *Decifra* serve a visualizzare e decifrare i file cifrati presenti nella cartella
`VPSS\users\username\ciphertexts`
Sia `username` il nome dell'utente loggato. La decifratura avviene utilizzando la Chiave Segreta di decifratura `username_secret.k` presente nella cartella
`VPSS\users\username\secret_keys\ABE_sk`

5.4.2.1 Visualizzazione dei file

I file cifrati dell'utente `username` contenuti nella cartella
`VPSS\users\username\ciphertexts`
sono visualizzabili tramite una tabella costituita dalle seguenti colonne

- `File`, contenente il nome del file cifrato
- `Autorizzazione`, contenente tre tipi di messaggio
  - `Autorizzato`, se gli attributi dell'utente soddisfano la policy associata al file cifrato
  - `NON Autorizzato`, se gli attributi dell'utente *non* soddisfano la policy associata al file cifrato

  - `Obsoleto`, se il tempo in cui è stato cifrato il file è minore del tempo attuale del sistema; in questo caso l'utente non sarà in grado di decifrare il file.

- `Policy`, contenente la policy associata al file
- `Cifrato da`, contentente il nome dell'utente che per ultimo ha cifrato il file
- `Chiave Pubblica`, contenente il nome del file che contiene la chiave pubblica utilizzata per cifrare
- `Livello sicurezza`, contenente il livello di sicurezza della cifratura
- `Gruppo`, contenente il nome del file che contiene il nome della curva ellittica utilizzata
- `Tempo`, contenente il tempo del sistema in cui il file è stato cifrato

La tabella appena descritta si aggiorna automaticamente al click del tab Decifra, oppure può essere aggiornata manualmente cliccando il pulsante `Aggiorna`.
Le righe della tabella possono apparire con tre colori

- NERO, se il file è decifrabile dall'utente
- ROSSO, se il file non è decifrabile dall'utente poiché i suoi attributi non soddisfano la policy del file
- ARANCIONE, se il file non è decifrabile dall'utente poiché la sua Chiave Segreta di decifratura ABE è stata aggiornata ad un tempo successivo al tempo in cui era stato cifrato il file.

5.4.2.2 Decifratura file

Per decifrare un file locale presente nella cartella
`VPSS\users\username\ciphertexts`
seguire le seguenti istruzioni

1. Cliccare sul pulsante `File...` per scegliere un file dalla cartella `VPSS\users\username\ciphertexts`
2. Selezionare uno dei file presenti e cliccare il pulsante `Open`
3. Cliccare il pulsante `Decifra`
4. Cliccare il pulsante `OK` nella finestra informativa che viene visualizzata

Se il file cifrato si chiama `[nome_file].[estensione].enc`, il file decifrato si chiama `[nome_file].[estensione]` e viene memorizzato nella cartella
`VPSS\users\username\plaintexts`
Se nella precedente cartella esiste già un file di nome `[nome_file].[estensione]`, allora al nome del file viene aggiunto il primo indice incrementale maggiore o uguale a 2, ad esempio `[nome_file]2.[estensione]`.

Maggiori dettagli

Durante la decifratura del file `[nome_file].[estensione].enc` avvengono le seguenti operazioni

1. Viene estratta la stringa di *metadati* (Sezione 6.7.1.1)
2. La password cifrata con lo schema ABE (Sezione 6.7.1.2) viene estratta nel file `password.k.enc`

3. Il file `password.k.enc` viene decifrato con la Chiave Segreta di decifratura ABE `username_secret.k` nel file `password.k` contenuto temporaneamente nella cartella
   `VPSS\users\username\secret_keys\AES_sk`
4. Viene creato un file temporaneo `ciphertext.temp` contenente la cifratura AES.
5. Dal file `ciphertext.temp` vengono letti il *salt* e l'*IV*
6. Utilizzando il contenuto del file `password.k` come password e il salt e l'IV appena letti viene generata la chiave simmetrica AES di decifratura.
7. Il file `ciphertext.temp` viene decifrato nel file
   `[nome_file].[estensione]`
   memorizzato nella cartella
   `VPSS\users\username\plaintexts`
   Viene aggiunto un indice in coda se il nome è già esistente.
8. I file `ciphertext.temp`, `password.k.enc`, `password.k` vengono eliminati

5.4.3 Tab *Trasferimento file*

Il tab *Trasferimento file* permette di

- caricare file locali sul Server di Archiviazione associando ad essi delle parole chiave cifrate (Sezione 5.4.3.1)
- effettuare ricerche per parola chiave tra i file cifrati presenti nel Server di Archiviazione (Sezione 5.4.3.2)
- scaricare uno o più file dal Server di Archiviazione (Sezione 5.4.3.3)

5.4.3.1 Upload di un file

Per caricare un file locale cifrato dall'utente sul Server di Archiviazione , seguire le seguenti istruzioni

1. Cliccare sul pulsante `File...`
2. Selezionare uno dei file presenti nella finestra che viene visualizzata
3. Cliccare il tasto `Open`
4. Aggiungere un elenco di parole chiave nel campo `Aggiungi parole chiave:`. Le parole chiave devono essere costituite da caratteri alfanumerici e devono essere separate da una virgola. Il carattere spaziatore non viene considerato. E' possibile non associare alcuna parola chiave al file cifrato.
5. Cliccare sul pulsante `Carica sul cloud`

Se nel Server di Archiviazione è già presente un file con nome identico a quello caricato, a quest'ultimo viene aggiunto il primo indice progressivo libero maggiore o uguale a 2.

Maggiori dettagli

I file locali vengono caricati sul Server di Archiviazione tramite il protocollo FTP.
I metadati relativi al file (Sezione 6.7.1.1) vengono caricati su un database MySql nel Server di Ricerca, insieme alle parole chiave cifrate. Ciascuna parola viene viene cifrata in modalità CBC con la cifrante AES-128, con IV e chiave simmetrica da 128 bit definiti nel file `search.k`.
Le parole chiave non sono mai rivelate al Server di Archiviazione, mentre il Server di Ricerca non ha mai accesso il contenuto cifrato dei file caricati.

5.4.3.2 Ricerca cifrata di un file

I file presenti sul Server di Archiviazione sono elencati nella tabella `Contenuto cloud:`. E' possibile effettuare delle ricerche inserendo come filtro una formula Booleana in forma normale disgiuntiva senza la negazione nel campo `Filtra per parola chiave:`.
Il simbolo AND logico è rappresentato dal carattere speciale `&`.
Il simbolo OR logico è rappresentato dal carattere speciale `|`.
Il simbolo AND ha priorità sul simbolo OR.
Alcuni esempi di formule ammissibili sono le seguenti

```
parola1 | parola2
parola1 & parola2
parola1 & parola2 | parola3
parola1 & parola3 | parola1 & parola2
```

Per effettuare una ricerca tra i file del Server di Archiviazione seguire le seguenti istruzioni

1. Inserire una formula ammissibile nel campo `Filtra per parola chiave:`
2. Cliccare sul pulsante `Aggiorna`

Il risultato della ricerca viene presentato come elenco nella tabella `Contenuto cloud`.
I file elencati sono tutti e soli i file il cui insieme di parole chiave associato soddisfa la formula inserita come filtro di ricerca.
La ricerca è key sensitive.

Maggiori dettagli

La struttura della formula Booleana inviata al Server di Ricerca rimane in chiaro. Tuttavia le foglie della formula sono cifrate tramite la Chiave Segreta di ricerca.

5.4.3.3 Download di un file

Per scaricare uno o più file dal Server di Archiviazione in locale seguire le seguenti istruzioni

1. Selezionare uno o più file nella tabella `Contenuto cloud`. Per selezionare più di un file tenere premuto il tasto `Ctrl` e cliccare con il mouse sulla riga relativa al file desiderato.

2. Cliccare il pulsante `Scarica selezione in locale`

I file scaritati vengono memorizzati nella cartella
`VPSS\users\username\ciphertexts`
Se viene trovato un file con nome identico al nome del file scaricato, a quest'ultimo viene aggiunto il primo indice progressivo maggiore o uguale a 2.

5.4.4 Tab *Visualizza contenuto cartelle*

Il tab *Visualizza contenuto cartelle* permette la visualizzazione e l'apertura dei file contenuti nelle seguenti cartelle

- `VPSS\public_parameters`
  La cartella contiene i file
  - `public.k`
  - `group.g`
  - `time.t`
- `VPSS\users\username\secret_keys\ABE_sk`
  La cartella contiene il file
  - `username_secret.k`
- `VPSS\users\username\plaintexts`
  La cartella contiene i file in chiaro.
- `VPSS\users\username\ciphertexts`
  La cartella contiene i file cifrati.

Si osservi che il promo blocco di file (*public.k*, *group.g*, *time.t*) contiene informazioni pubbliche del sistema, comuni a tutti gli utenti; le successive informazioni sono invece specifiche dell'utente loggato.
Per visualizzare il contenuto di un file cliccare due volte sul nome del file.
Per aprire una cartella cliccare due volte nell'area di colore bianco relativa alla cartella interessata.
Per aggiornare l'elenco dei file visualizzati cliccare il pulsante `Aggiorna`.

6 Oggetti del sistema

6.1 Chiave Master

La *Chiave Master* è il segreto custodito dall'Authority, dal quale genera Chiave Pubblica e Chiave Segrete di decifratura.
Chi è in possesso di questo segreto è in grado di decifrare qualsiasi file cifrato con la Chiave Pubblica generata partendo da esso.
La sua dimensione è fissa.

6.1.1 Formato Chiave Master

Il nome del file contenente la Chiave Master è
`master.k`
ed è contenuto nella cartella
`VPSS\demo_abe\authority\master_keys`
Un esempio di una Chiave Master per una sicurezza da 112 bit è il seguente:

```
eJyVVMtu20AM/BVBZx2Wq31w+ytFarhBkB58KOC2QBH437MzJDe55mBL4pszJN/21/zjevv967p/29
72y+X5dr3fL5f5tf/8/+flvh/blP673v6+UPq9pmOremyKZz82yXn+pYE3maL5pWV+yJT0KejnsbU2
n7CV+dfrsY2pLPO9QtHgD6F6tCouaTCfwcoJTYKUySI+M4rMALVG/mJuFS4yXZThm2mQAlpJqGxEKr
VqmJz2yAVJV/vBhwopbtaQMJ3WbBnWEstT9RdIYAbErFL01Gu8JGuOqoUOYNUp0OrZevZEeGnDna19
6VGSAC01+CnR0xq0oMNNunyyHd3pWixKtJojOIDokQ+GiyTSVy0J+OlOPp7UJeMeWVA6ORRXWvnA3W
DzMQBphk82ZzpUZxEatMWsp6Mikg2sMrwBkQBLnWhOJz2b2aKmkXxQUQUHdDWNKCo+P4Xqp8fcg1f5
2qqgJKwKWtPTmdbglAuSPEt37kh9tm+bc2AD4EtwyPJIQ+pL1GzUyDiHJWgy6485kYXbaSjipz62CM
EBdB6a46rJ/fHRVjHFPIfXzmUZNm3cKwOzeczmbNTILikWA2vQQg9DgA6ymh8R28zAhWtR1iZIiDTS
1bhBTi36R3/EMaaj+V4giOYoYB2I89Om2NlBDh6RZP0VXwcUyf5HzJvENSoxTna9ckxlTh9N44iyx+
THkU7GrZh6rOvg9whjwnX3A2lrn6IG33Ro2PaIHYjd4sFSOzuI0/38coaacVBj/9nO8EPA5vO6xL58
lRfx6fF4B5ymL3w=
```

6.2 Chiave Pubblica

La *Chiave Pubblica* è un dato conviso da tutti gli utenti del sistema e serve a cifrare un file in chiaro rispetto ad una policy sull'universo di attributi.
La Chiave Pubblica è generata dall'Authority tramite un algoritmo randomizzato a partire dalla Chiave Master.
La sua dimensione è fissa.

6.2.1 Formato Chiave Pubblica

Il nome del file contenente la Chiave Pubblica è
`public.k`
ed è contenuto nella cartella
`VPSS\demo_abe\public_parameters`
Un esempio di una Chiave Pubblica per una sicurezza da 112 bit è il seguente:

```
eJyVWMtuJDcM/JXBnBJgDpJaIqn8SrBreBeGc/AhgJMAwcL/niZZJfXenMN4d7olio+qIjU/7q/1/t
vtx/3p6fvb8/v709P57f7t379e3u+P2/n0n+e3v1/i6e99Pm7DHjeRx83q49aPx63Wcf4p5zfT83N+
UfWn5ys9l/uWWs8/5mtbO58euWx0LnVr5kYMlmo51v98fyvnmefLiX99azyc5/7hR0983EI9HwiP9v
0Whpq/arkeTpf0pFuG4hb0XGHuGff4WW5WDNb8ge/QMO+BFAShkY7TJXG3NJe4Jyq+VJAWf5OONngb
WSuXNIpcPVZkylM4Wn5qPR/Kuc8EXyLLmTSPzmivx1GePcuzPRLflWZiWWcZwoRmYt2RcGKifDLwNi
vl57m9qMQYiCUSEGa74vDIs2UqImP+1Ohy7IxYS/nJjU6LfqSnUEfmwreOgzsncSgLMzgvkyxwXogr
ByE9sIbKhDuFro8DDgTim4f+5eNkw2v9+vx/yaJMbuQpwyooeuKwshCOAa+SbnRoQtLhGHUriS6SyK
HtZVFkwRkSeIw0T0BjoBJTkZ3YslYAw0aqDRaDNEVuwb6oWtSjAK2GA8OU23S0KtxLiLldd3ogcluo
LLk0kEQ8dEpIomQgE6EwKI/h46CKKjYYSpQd1BTNlIbpeFXtcnrAJ3jrIFi4TDjCGQ8zEdaAK8ZwLM
zY5XVAtFIDgVk/elKQsigHlREY86RNctgLmsLCvMjCi3unCHsww5mpQpF1fksm0g8KReqQEKXwFsqS
85kqSCV0yymh5SdWGHMN+nt0F4q8/PL6+uvX57c///g0U/ykAX3ImFF5YxtwuZqAPpA2QZVjtwYPUI
TomYn3gLoldtxdd3USGUrY11X11ogB4ImfgbQG2IIChRgrSVI/OzSpVSTKn85CLDUkDBDyxHmyPQQa
DpXy7YxtqUf0kEoPtfFVZwSVEFm9M1gbngLFIZoQUEE3MF0r0Ydda0heJfUg+cSXlyw9qrvVDaRa2c
LDEjpBBFNyFyWCuoR+v46JhJK0ydWBWCNhSpb3C587gtm6w2ZmmEXQn3pSY8CZALMJ0TaBtEVEIfvZ
3KxefAF/ZLluNNTZYRtjayB5sEuQt0qE7Pzi+JThg/q11HetLkBXzh2dQRpy0LNMwspAnhLhZSVVcl
9WUxGMoDKrrStFpewenNRksDI2AzNzjeYbPDguIeRQ1lEzwZQhrOrq/tnkSQtFnfpVLtp1jkpFH5nZ
wbro2CgE2ljXAvROJi8lOvrfQYjUJfIIzMiYFEW23N0k2fC8QBHa4FzTQASOTmkTgi2kermeFuNYh2
RMxKYZfsTIjMbcS2Gzx55tFjSidwJhIVqaymOY+rIzdPDpmsNRWKBCqdELc1Yzt3wr7k7Nsal9uhUU
DE11t82c4Ru6UWNTnIUFPwBLzlJMdRCoLV3slwnW0BPdvij5sATt2FOXKUd99uDCmcTQMaMHh4pwMF
9Xj2RrjudKMajI3+CQEthtS7upfNl0BTPOalM82pS3BhQm4UxwFhaaxObIAKAihfEqprJKwSLYU3cw
DkzwIQMl7WKuwG0wib/byfUSsgZqbReVqOSWUM5kMqZ1XVsqgknOIE8CD5Vq2tFacTPws2MGR9MTuz
TIgdurksENFDBOZbzjxmChROEuAoeimFPYSionYQUXDV0ggBrQ9XAHRWTsm0X7/M1ikWTdnnizQyk5
rkSoHSOpIj9DLjNJJ476RaUwVU82iyw5mpVNDli8kqwbvhJ1k5Jd26ZX0nO1K/S1rhveEwNwkB+AWv
0GUJgcpApO3YPyarYJ4LpZToTCKV6uOYjNyavRpTnLHn3X8M07qO5xymjMePMc+MTAY6QclT+XQLpl
EYwTCg0AZLxwkLAczcaeAS6D5cJuHskh1w4WnDeIdfOXSSbyh4IAr9Awk8PjTNkPlDcO/tTB09YEFb
xfN85B6SCGDLeqgfs+r25KeSnxO8iXj4//ALA6cvA=
```

6.3 Curva Ellittica

Il livello di sicurezza dell'intero crittosistema e la sua efficienza sono determinati dalla scelta di un oggetto matematico chiamato *Curva Ellittica*.
La Chiave Master, la Chiave Pubblica, e le Chiavi Segrete di decifratura sono definiti tramite tale curva ellittica.
Affinché i protocolli ABE utilizzati siano applicabili su tale curva deve essere definibile una mappa bilineare.
Notiamo che le curve ottimali per protocolli basati sul Logaritmo Discreto non sono ottimali per crittosistemi ABE, e viceversa.

6.3.1 Formato del file Curva Ellittica

Il nome del file contenente il nome della curva ellittica utilizzata nel protocollo ABE è
`group.g`
ed è contenuto nella cartella
`VPSS\demo_abe\public_parameters`
I possibili contenuti del file `group.g` sono i seguenti

- `SS512`
- `SS_e_R224Q1024`
- `SS_e_R224Q2048`
- `SS_e_R256Q3072`
- `SS_e_R384Q8192`

con rispettivi livelli di sicurezza 80, 112, 112, 256, 384.
Il significato di tali nomi è deducibile dalle informazioni contenute nel file `pairingcurves.py`.

6.4 Tempo del sistema

Il *Tempo* t del crittosistema si riferisce alla t-esima Chiave Master generata da parte dell'Authority.
Ad ogni generazione (2.4.1.1) il tempo incrementa di uno e cambiano anche la Chiave Pubblica, la Curva Ellittica utilizzata, le Chiave Segrete di decifratura. Inoltre tutti i file nel Server di Archiviazione vengono ricifrati con la nuova Chiave Pubblica.
Alla prima generazione il tempo è settato al valore `1`.

6.4.1 Formato del file Tempo del sistema

Il nome del file contenente il tempo attuale del sistema è
`time.t`
ed è contenuto nella cartella
`VPSS\demo_abe\public_parameters`
Il file contiene una stringa rappresentante un numero intero n, il quale indica che la chiave pubblica attualmente in uso è l'n-esima chiave pubblica generata dall'Authority.
Se per esempio la chiave in uso fosse la 15-esima chiave generata, il contenuto del file sarebbe il seguente

```
15
```

6.5 Chiave Segreta di decifratura

La *Chiave Segreta di decifratura* è un dato segreto assegnato a ciascun utente del sistema a cui sono stati riconosciuti degli attributi da parte dell'Authority, e serve a decifrare un file cifrato.

La Chiave Segreta di decifratura contiene intrinsecamente gli attributi dell'utente.
Essa è generata dall'Authority tramite un algoritmo randomizzato a partire dalla Chiave Master.
La sua dimensione aumenta linearmente con il numero di attributi dell'utente.

6.5.1 Formato Chiave Segreta di decifratura

Se il nome dell'utente in possesso della Chiave Segreta di decifratura è `username`, allora il nome del file contenente la Chiave Segreta di decifratura è
`username_secret.k`
ed è contenuto nella cartella
`VPSS\demo_abe\users\username\secret_keys\ABE_sk`
Un esempio di una Chiave Segreta di decifratura per una sicurezza da 112 bit è il seguente:

```
eJx9VrtuHDEM/JXD1VeI2tUrXWqnCtwFxsEOXARw5bODBIb/PZrhUI4ROMXe7Wopajgckvtyvdr/On
46vBw/X19/Nd6dzz9vH57vz+f59G0fp0Ppp0Od/6OdDr2eDljr5XRo83+fa5bmw4BRj4X50xJubG7f
5rXPB5sPfXdf3GNp6HV982wpz81YmA5682skGcAxfKUkH3WutuxgGs7vvttsmrXpu5sbcMEsC0gx3V
QAzjrLUnVXAIw3DUcUR1ZL4DacbjDLHnXv8o1IeGpzOARaeOh8Ks0Z4F73kjYRa6JrJLmii+pvcTk5
1c+wnD0JhN5abA5queLBFlkXQQIasGTZdD69uo3FOtlK+X2mG91HLs2C51L8ch43KcDPhzl84NhmsT
9lpX9X/DTe4xwoRffkg5oI+iE1XPumqEknUkBCLHIyHDBMERfiLyn0o2jwAAlBk+Cs1pvTYZbA94fb
y4UlcLz7/XR/Ob6+zvUv/xYIPLJA6sqoCScZYaBMVpIw8QockUzbxHDyvJYkqeyhRtZGdzWGumoQTy
vkixJLXaT27LzBG/7BVNc6fC29MGGscVlzu4t2l49IYhFECBhwKW/rQgJ4CHF0iYp4i0q3qYq61zvl
Z1uoPofiJf+ASQgtzC0aRhUzNQgkXnACJvdoNyzlJvAkCukB+h4VtUVozVOy+lBTEEgYW0CP/jAEcV
danYGlwhodjMyqVobgU/4WNKbwgM1NcChy1h7rOoIrq4uoKSAB9MC3xSEXdUnvAN0t2K2HHx67eBW5
3RRrCRnllXVzlUb6avmoOOby1ce1wVEQ/XhEu6TSbCnRf1pUc/K0o6EVZbWpHwNoVwtHuKVJ+1jsJV
poXRkqLqm3I4baILFEA+xRequEeiSuRlGQzC0CiOws8TZpkDPFYoZpT0wngYomO9SJILF3rWmNt5iZ
3hvU7mGKF14NY2mpLWaLptiIWaxe2CW1ErW3rxJLghMdLHqHF3VTHYQOERxn4hoxqsas0soxdqu0CO
el/RWFaFjDtb4BKPpaQMZxUa8hj6Z56FO8azhatBaIgb0rWhxTDxt+KnQ/bkS9Ek0RRMHkUAgxxPjt
+/IXHYwjS13pv/Vx+/T0+OPuGY+zNI6Xp8dP/s118/oHCVLJ+w==
```

6.6 Chiave Segreta di ricerca

La *Chiave Segreta di ricerca* è un dato segreto assegnato a ciascun utente del sistema e serve ad effettuare ricerche in maniera cifrata, in modo che il Server di Ricerca non conosca il significato delle parole chiave ricercate.
La Chiave Segreta di Ricerca è uguale per ogni utente e non varia al variare del tempo del sistema.
Essa è generata una volta per tutte durante il setup del sistema.
La sua dimensione è fissa.

6.6.1 Formato Chiave Segreta di ricerca

Se il nome dell'utente in possesso della Chiave Segreta di ricerca è `username`, allora il nome del file contenente la Chiave Segreta di ricerca è

`search.k`
ed è contenuto nella cartella
`VPSS\demo_abe\users\username\secret_keys\SEARCH_sk`
Il contenuto di questo file è suddiviso in due strighe da 16 caratteri esadecimali

- *IV*
- *chiave simmetrica*

separate dal carattere "`:`" ("due punti").
Un esempio di una Chiave Segreta di ricerca per una sicurezza da 128 bit è il seguente:

```
0000000000000000:0123456789abcdef
```

Notiamo che questo file, e quindi la Chiave Segreta di ricerca, è identico per ogni utente e non varia al variare del tempo del sistema.

6.7 File cifrati

Ogni tipo di file in chiaro può essere cifrato dall'utente utilizzando la Chiave Pubblica ed una policy.
Il file cifrato ottenuto ha dimensioni linearmente proporzionali al numero di foglie della formula Booleana rappresentante la policy.

6.7.1 Formato del file cifrato

Il contenuto di un file cifrato è suddiviso in tre campi:

1. metadati
2. cifratura della password
3. cifratura del file in chiaro

I tre campi sono separati dalla stringa
`___FILESEPARATOR___`

6.7.1.1 Campo metadati

Il campo *metadati* contiene i metadati, in formato leggibile, relativi al file cifrato. I metadati contenuti in questo campo sono i seguenti

- tempo del sistema
- cifratore del messaggio
- livello di sicurezza della cifratura
- percorso del file `group.g`, che definisce la curva utilizzata per la cifratura ABE

- percorso del file public.k, che definisce la chiave pubblica
- policy utilizzata per la cifratura

I precedenti campi sono separati dalla stringa
&&

6.7.1.2 Campo cifratura della password

Il campo *cifratura della password* contiene la cifratura della password generata durante la cifratura del file (Sezione 5.4.1.2).
La cifratura della password avviene tramite uno schema ABE.
Il formato di questo campo è una stringa di caratteri ASCII.

6.7.1.3 Campo cifratura del file in chiaro

Il campo *cifratura del file in chiaro* contiene la cifratura AES del file in chiaro utilizzando, come descrtitto nella Sezione 5.4.1.2.
Il formato di questo campo è una stringa di caratteri esadecimali.

6.7.1.4 Esempio

Un esempio di contenuto di un file cifrato è il seguente

```
TIME=1&&UTENTE=utente1&&SECLEV=80&&GROUPPATH=C:\Users\ema\Desktop\VPSS\demo
_vpss\public_parameters\group.g&&PKPATH=C:\Users\ema\Desktop\VPSS\demo_cpa
be\public_parameters\public.k&&POLICY=ATTR1___FILESEPARATOR___eJyNVctuGzEM/BVj
zz5IWj1zK5IvKHILCsNJfTBgoEW8KRAE/vdqyKHWBtq0h31IosThDEl9TPfT3eZj+vL4+NXL3273a3
96O+x2ffQU23aT6nZT/HbjQ3+lst001weuv1LoKwGDPlubrnoXu0n/KUX31f5N3brQoKT+5P50O+8z
J2YM8ON0V7EjI717ePUVDm6HIRCb99gz5jGKs86ILxe5VL0F4Q0CQuvfiFU80Q6GH0SgHuSFcwATQV
ZDAA84gb6bxuhd0OAV1ghUlsgD0NR5jTrbAfLK3Sr7b9tNF+bltD+fRZjp+X05nKfLpc8/fCYgfCcL
qiqdgjd5AmpVFYA0qh8Gs3GWYBa4qWYVHPRoIH3QgDLrJNyBQ+wFa2pE0ZUe4x1bxGcchIgbxz8wnJ
JSExuP8a7RIUGmmWfGyqSEsEp9UcB4kKlwL6qv5sZ0buYjUnvfz83FbIAXOOGZlMgaT66BvoUkQNMw
/k+/e/f3usNucCnPEKgYY8g1S1nFH6xWnQYC9gRnnJm5Ep6bdUkyW5CPQvQ8AYGjAItpJGZSQ64RRS
yDilnJRVoBNEiXaoHJyARshKY8KxGb7Ba2ERAsoRW+SLaSDLAQzyakJRa1fHLmRHK3/Lg1PXXTcK5l
6lgVmWvVzvi3dFButxxP3w9/qDqv8glaKz2N3lqJQM8koDZL+sRlaaDtyqSZxI4xRXIGcoVxxzwug1
qvBzazMqEECXiTGmMni8ZPqVfxF2PXeaMpsDxUtaxeJV3wg9BLs5Rha0vMDImkMO80YbPpGpSlzFhL
uVJCV9cmwNtE5fSjbayHWZmgl0pg4TqRou3NIwlIiNr5G2emo5BaqZYlCtwVVokgSXYRlYE00ZtmoF
05yepQS8BqRbqHFljk/TD6VlB/1S48CArOwZu0JiR1tn7ODqkxRpOxKfnSFyTYwmoLJo+1j0azccWJ
z2rJEJmDEhFQfFoq+2V5PT6/LSiWp+m8vN7phYUtP3+cji/vsF/nL78BdrqqBA==___FILESEPARAT
OR___2403e824f2324d59a106bad21754f0342b78af17c773491cf5fdb0c9f393d886894b5da25
5b8b0fa7d432440d501c676
```

Bibliografia

[1] Joseph A. Akinyele, Christina Garman, Ian Miers, Matthew W. Pagano, Michael Rushanan, Matthew Green, and Aviel D. Rubin. Charm: a framework for rapidly prototyping cryptosystems. *Journal of Cryptographic Engineering*, 3(2):111–128, 2013.

[2] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pages 321–334. IEEE, 2007.

[3] B. Kaliski. Pkcs #5: Password-based cryptography specification, version 2.0. Accessed December 20, 2014.

[4] Brent Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Public Key Cryptography–PKC 2011*, pages 53–70. Springer, 2011.