

Piattaforma AlmaChannel e laboratori virtuali

Tecnologie per la Sicurezza L-S
AA 2005-2006

Anna Riccioni
anna.riccioni@gmail.com

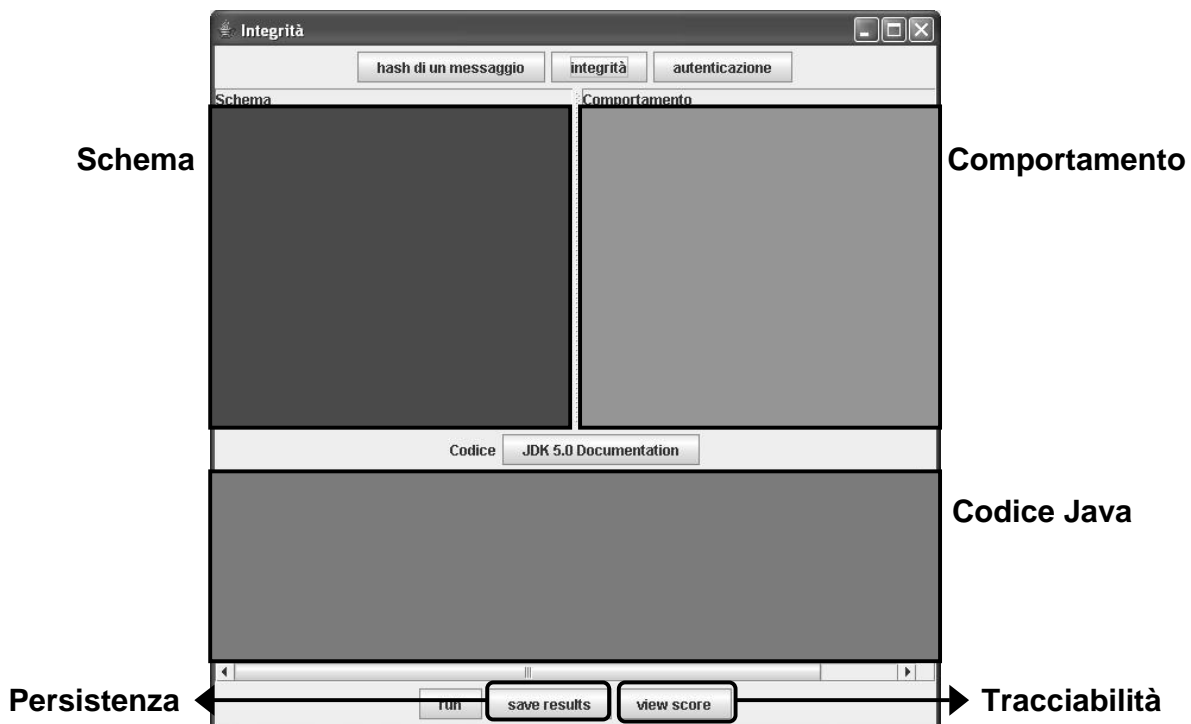
Laboratori virtuali

- Supporto alla didattica tradizionale
- Simulatore come ambiente di lavoro
 - esemplificazione di situazioni reali
 - riproduzione di meccanismi e servizi studiati sotto forma di schemi
 - possibilità di azione e di esecuzione di prove mirate
 - verifica dei concetti teorici studiati
 - sperimentazione

vlab

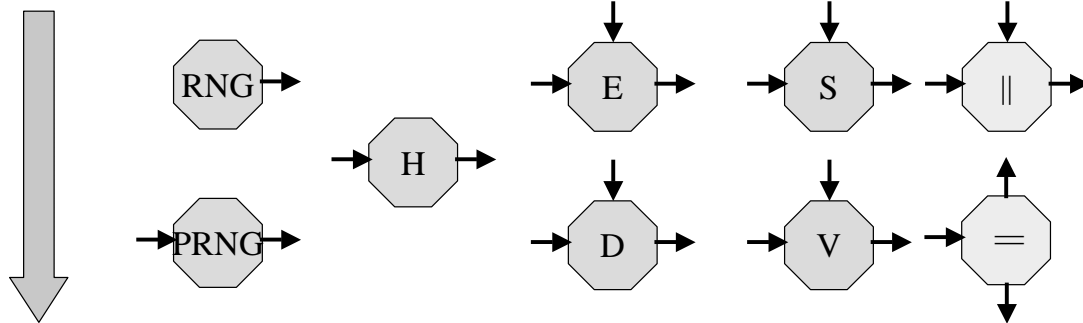
- Framework per l'esecuzione di esercitazioni
- Obiettivi:
 - riprodurre gli schemi visti a lezione
 - costruire il codice Java associato, in funzione dei parametri impostati
 - rendere disponibile un contesto già pronto per l'esecuzione di prove e la sperimentazione di concetti teorici
 - semplificare l'analisi e interpretazione dei risultati grazie ai dati sull'esecuzione

vlab



Esercitazione

- Meccanismi



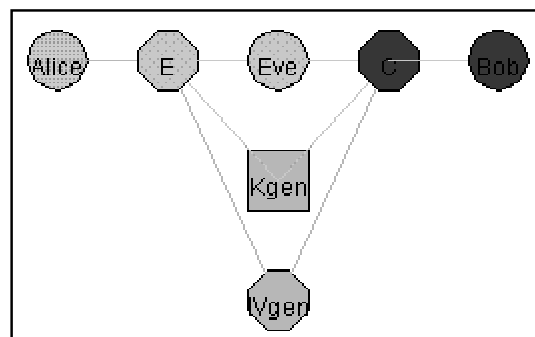
- Componente

- input
- output
- funzione



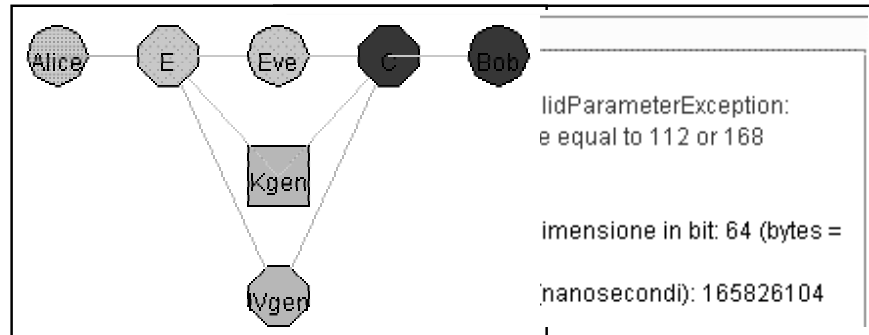
- parametri
 - funzione specifica
- esecuzione
 - codice Java
 - comportamento

Codice dei colori: componente



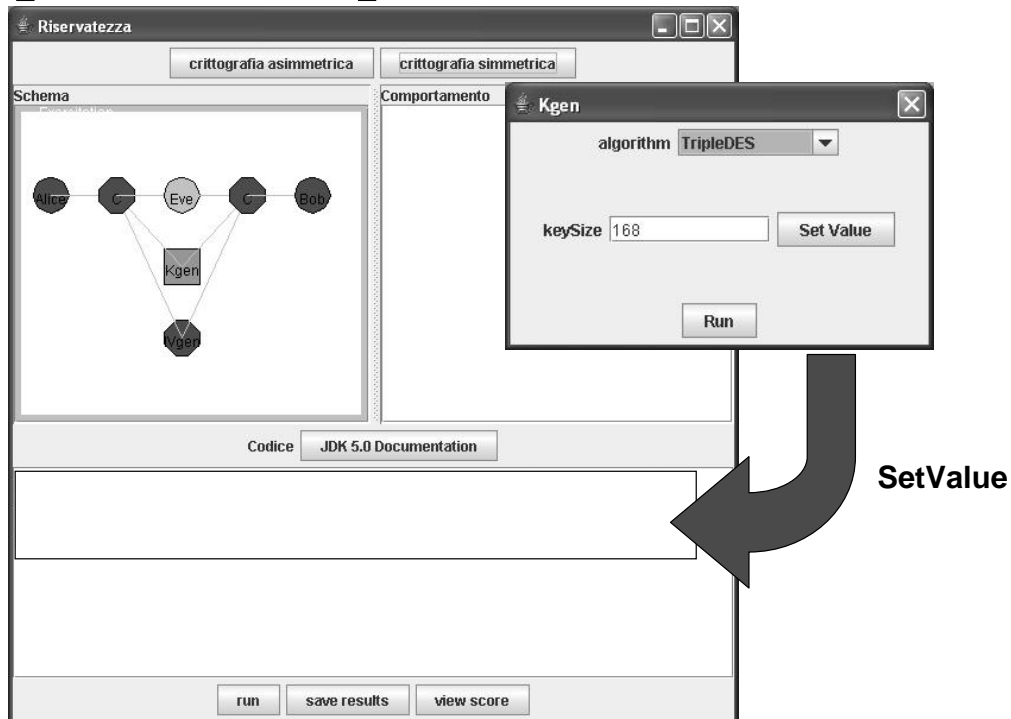
- Rosso: parametri non impostati
- Giallo: input non disponibile o non letto
- Verde: componente eseguito
- Grigio: attori coinvolti nel processo descritto

Codice dei colori: connessione



- Verde, a valle di un componente verde: esecuzione andata a buon fine
- Giallo, a valle di un componente giallo o rosso: input non disponibile
- Giallo, a valle di un componente verde: esecuzione terminata con un'eccezione

Impostazione parametri



Impostazione parametri

The image shows a screenshot of the 'Riservatezza' application. The main window has two tabs: 'crittografia asimmetrica' and 'crittografia simmetrica'. The 'Schema' tab is active, displaying a diagram with nodes for Alice, Bob, Eve, and Kgen. Alice and Bob are connected to Eve, and Eve is connected to Kgen. A 'Comportamento' tab is also visible. Below the schema, there is a code editor with the following code:

```
KeyGenerator Kgen = KeyGenerator.getInstance("TripleDES");
Kgen.init(123);
Key outputKgen = Kgen.generateKey();
```

At the bottom of the code editor are buttons for 'run', 'save results', and 'view score'. A separate 'Kgen' dialog box is shown, with 'algorithm' set to 'TripleDES' and 'keySize' set to '123'. A 'Run' button is at the bottom of the dialog. An arrow labeled 'Run' points from the dialog to the 'Comportamento' tab in the main window.

Vincoli di precedenza

- Esercitazione:
sequenza ordinata di componenti collegati
- Esecuzione dei componenti:
 - componente eseguibile se tutti i parametri sono stati impostati e tutti gli input sono disponibili
 - un componente non può essere eseguito prima di quello a monte nello schema
- Configurazione dei componenti:
 - nessun vincolo nell'ordine di impostazione dei parametri di componenti diversi
 - alcuni parametri vanno impostati prima che vengano definiti i dati a cui fanno riferimento

Vincoli di precedenza

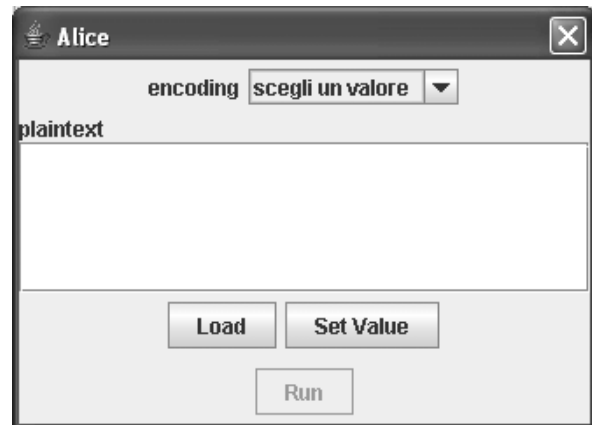
- Componente di input (Alice)

- parametro Encoding:

- UTF-8
- UTF-16
- HEX
- BASE-64

- dato Plaintext:

- composto nell'area di testo
- caricato da file



Vincoli di precedenza

- Testo composto all'interno della text area:

- al momento dell'esecuzione del componente viene interpretato in funzione della codifica specificata

- Testo importato da file:

- al momento del caricamento viene visualizzato all'interno della text area e quindi convertito in stringa in funzione della codifica specificata
- per evitare perdita di informazione occorre prima selezionare un'opportuna codifica, soprattutto nel caso in cui si importi un file non UTF-8 o UTF-16

Encoding

- Codifiche disponibili:

- UTF-8 stringhe, file di testo
- UTF-16
- HEX file binari, file in formati complessi
- BASE-64

- HEX e BASE-64 consentono di rappresentare in formato testuale il contenuto di byte che le codifiche ASCII o UTF associano a caratteri non stampabili

HEX

- Codifica esadecimale:

- anziché rappresentare un intero byte, se ne considera la metà
- le 2^4 possibili combinazioni sono rappresentate dai caratteri [0..9] U [A..F]
- usando un carattere ASCII per ogni 4 bit si codifica una qualsiasi sequenza di byte in modo stampabile, ma se ne raddoppia la dimensione

BASE-64

- Codifica in BASE-64:

- anziché considerare un byte alla volta, se ne considerano 3

| | | |
|----------|----------|----------|
| 01010101 | 00000000 | 11111111 |
|----------|----------|----------|

- i 24 bit che compongono i 3 byte possono essere suddivisi in 4 blocchi da 6 bit l'uno

| | | | |
|--------|--------|--------|--------|
| 010101 | 010000 | 000011 | 111111 |
|--------|--------|--------|--------|

- un blocco di 6 bit ha 2^6 possibili configurazioni, ognuna delle quali è associata, nella codifica BASE-64, ad uno dei 64 caratteri stampabili nell'insieme $[A..Z] \cup [a..z] \cup [0..9] \cup \{+\} \cup \{/ \}$

BASE-64

- una codifica in BASE-64 trasforma la sequenza di byte di partenza in una nuova sequenza di byte, leggibile in forma testuale, ma la cui dimensione risulta incrementata di un terzo
- poiché si considerano 3 byte per volta, nel caso in cui la sequenza di byte di partenza non abbia una lunghezza multipla di 3 occorre utilizzare un "padding":
 - un eventuale blocco in BASE-64 incompleto viene riempito di "0" fino a raggiungere la dimensione di 6 bit
 - eventuali blocchi da 6 bit mancanti vengono sostituiti dal carattere speciale "="

BASE-64: esempio

H e l l o

| | | | | |
|----------|----------|----------|----------|----------|
| 01001000 | 01100101 | 01101100 | 01101100 | 01101111 |
|----------|----------|----------|----------|----------|

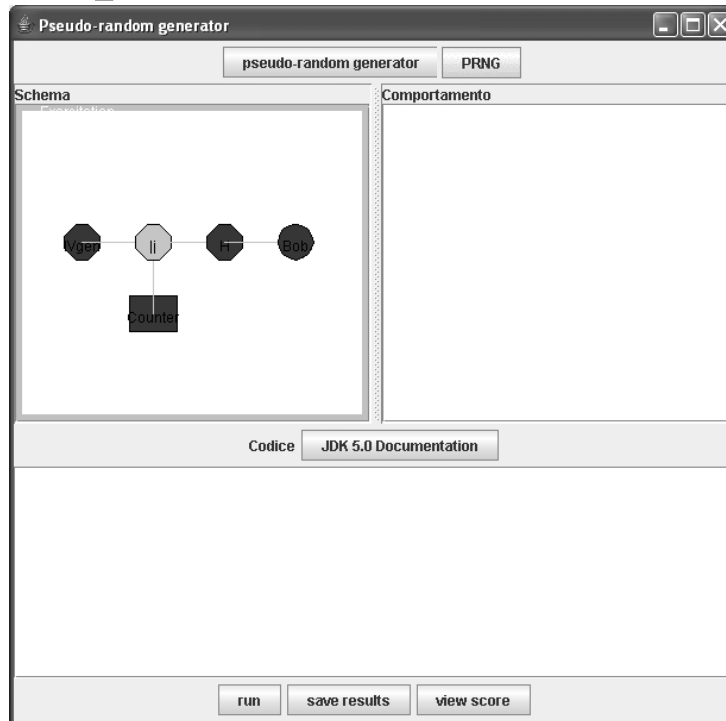
| | | | | | | | |
|--------|--------|--------|--------|--------|--------|--------|--------|
| 010010 | 000110 | 010101 | 101100 | 011011 | 000110 | 111100 | XXXXXX |
|--------|--------|--------|--------|--------|--------|--------|--------|

S G V s b G 8 =

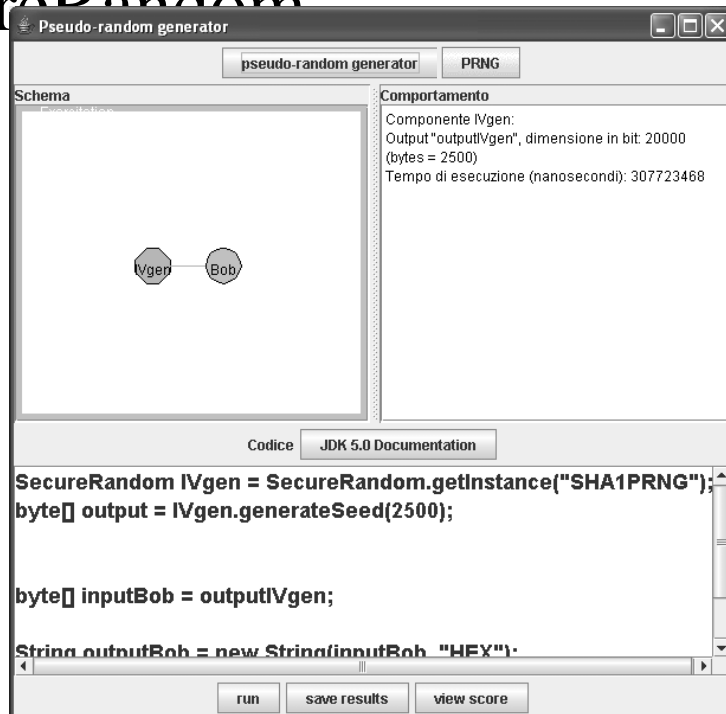
Esercitazioni disponibili

- Numeri pseudocasuali
 - generatore basato su SHA-1
 - classe `java.security.SecureRandom`
- Integrità
 - hash di un messaggio
 - verifica dell'integrità di un messaggio
 - verifica dell'integrità e autenticazione di un messaggio
- Riservatezza
 - crittografia simmetrica
 - crittografia asimmetrica

Numeri pseudocasuali: SHA-1



Numeri pseudocasuali: SecureRandom



Classe SecureRandom

- Creazione di oggetti SecureRandom attraverso il Factory Pattern

- i vari provider possono realizzare le proprie implementazioni, non necessariamente basate sull'hash SHA-1

- Istanziare un oggetto SecureRandom:

```
SecureRandom rand =  
    SecureRandom.getInstance("SHA1PRNG");
```

- consente di istanziare un oggetto SecureRandom basato sull'algoritmo specificato, se reso disponibile da almeno uno dei provider installati

Classe SecureRandom

- Istanziare un oggetto SecureRandom:

```
SecureRandom rand =  
    SecureRandom.getInstance("SHA1PRNG", "BC");
```

- consente di istanziare un oggetto SecureRandom basato sull'algoritmo specificato e nell'implementazione offerta dal provider richiesto. Se il provider non è disponibile viene sollevata un'eccezione

- Inizializzare un oggetto SecureRandom:

```
rand.setSeed(seed);
```

- inizializzazione forzata, basata su byte random precedentemente raccolti. In alternativa, l'oggetto può inizializzare autonomamente il proprio stato (meno efficiente)

Classe SecureRandom

- Generare byte random:

```
byte[] bytes = new byte[20];
```

```
rand.nextBytes(bytes);
```

- genera il numero di byte random desiderato dall'utente

- Generare byte di seed:

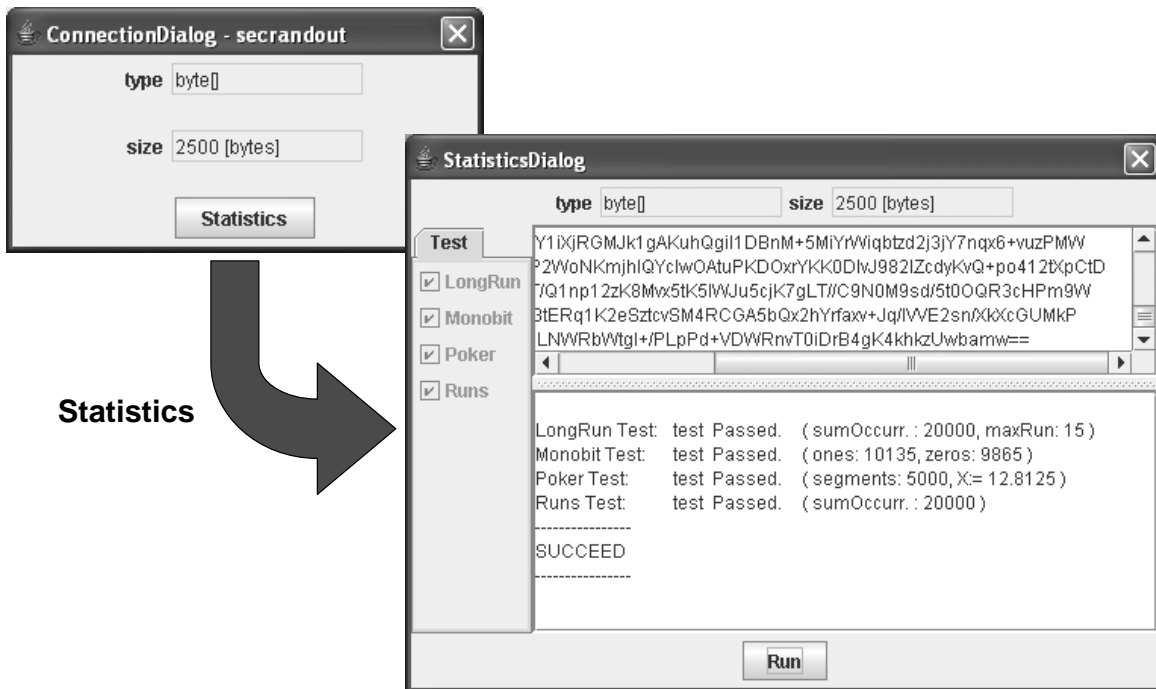
```
byte seed[] = rand.generateSeed(20);
```

- genera il numero di byte di seed richiesto, utilizzando l'algoritmo di generazione del seme che l'oggetto SecureRandom usa per inizializzare se stesso.

Test statistici

- Verifica della casualità di una sequenza di bit prodotta da un generatore di numeri casuali
- Standard FIPS 140-1 (NIST 1994):
 - campione di 20000 bit
 - superamento di quattro test
 - **monobit**: occorrenze di "0" e "1" circa equivalenti
 - **long run**: corsa più lunga di dimensione inferiore a 26
 - **runs**: occorrenze di tutte le corse di varie dimensioni (1, 2, 3, 4, 5, 6 e superiori) incluso in intervalli prefissati che rispecchiano i valori che si avrebbero in una sequenza casuale
 - **poker**: test del chi quadro per valutare se le occorrenze delle possibili stringhe di 4 bit approssimano il valore atteso per una sequenza casuale

Test statistici

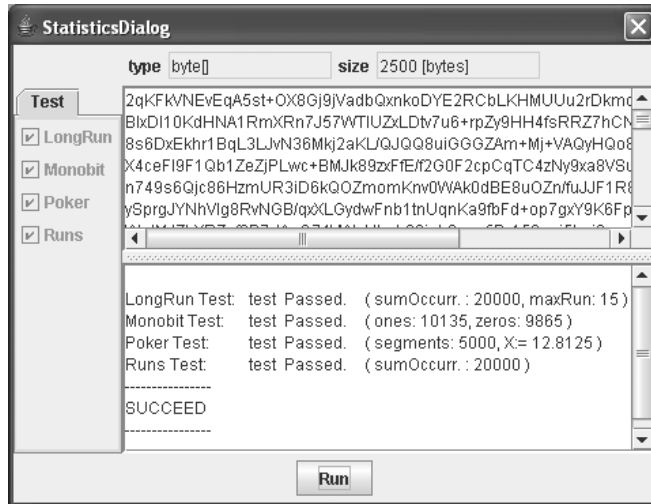


Test statistici

- Prerequisiti
 - standard FIPS 140-1: campione di 20000 bit
 - connessione che contiene un dato di almeno 2500 byte
- Quando utilizzarli
 - verifica dell'output di un generatore di numeri pseudocasuali
 - verifica dell'output di un'istanza della classe SecureRandom
 - analisi dei byte prodotti da un'operazione di cifratura
 - ...

Test statistici

- Come interpretare i risultati
 - confronto dei parametri caratteristici dei test con quelli considerati ammissibili dal FIPS 140-1



- long run: $X < 26$
- monobit: $9725 < X < 10275$
- poker: $2.16 < X < 46.17$
- runs:

| Lunghezza della corsa | Intervallo ammissibile |
|-----------------------|------------------------|
| 1 | 2315 - 2685 |
| 2 | 1114 - 1386 |
| 3 | 527 - 723 |
| 4 | 240 - 384 |
| 5 | 103 - 209 |
| 6+ | 103 - 209 |

Integrità: hash

The screenshot shows the "Integrità" application interface. It has three tabs: "hash di un messaggio", "integrità", and "autenticazione". The "integrità" tab is active, showing a diagram of a hash function where Alice sends a message to a hash function H, which outputs a hash to Bob. The "Comportamento" section provides details for the SHA-256 component: Input "inputH", dimensione in bit: 120 (bytes = 15); Output "outputH", dimensione in bit: 256 (bytes = 32); Tempo di esecuzione (nanosecondi): 116775. Below the diagram, there is a code editor with the following code:

```
byte[] inputH = outputAlice;

MessageDigest mDigest = MessageDigest.getInstance("SHA-256", "
byte[] outputH = mDigest.digest(inputH);
int digestLength = outputH.length

byte[] inputBob = outputH;
```

Integrità: verifica hash

Integrità

hash di un messaggio | integrità | autenticazione

Schema

Comportamento

Componente H:
Input "inputH", dimensione in bit: 120 (bytes = 15)
Output "outputH", dimensione in bit: 192 (bytes = 24)
Tempo di esecuzione (nanosecondi): 39390

Componente ||:
Input "firstInputConcatena", dimensione in bit: 192 (bytes = 24)
Input "secondInputConcatena", dimensione in bit: 120 (bytes = 15)
Output "outputConcatena", dimensione in bit: 312 (bytes = 39)
Tempo di esecuzione (nanosecondi): 1676

Componente H:

Codice [JDK 5.0 Documentation](#)

```
String plaintext = "Man Lo sono io!";  
byte[] outputAlice = null;  
byte[] inputAlice = plaintext.getBytes("UTF-8");  
  
byte[] inputH = outputAlice;  
byte[] secondInputConcatena = outputAlice;
```

run | save results | view score

Bob

encoding UTF-8

output

Confronto hash: true

Man Lo sono io!

Save

Run

Integrità: autenticazione

Integrità

hash di un messaggio | integrità | autenticazione

Schema

Comportamento

Componente IVgen:
Output "outputIVgen", dimensione in bit: 64 (bytes = 8)
Tempo di esecuzione (nanosecondi): 17002999

Componente ||:
Input "firstInputConcatena", dimensione in bit: 64 (bytes = 8)
Input "secondInputConcatena", dimensione in bit: 120 (bytes = 15)
Output "outputConcatena", dimensione in bit: 184 (bytes = 23)
Tempo di esecuzione (nanosecondi): 1676

Componente H:
Input "inputH", dimensione in bit: 184 (bytes = 23)

Codice [JDK 5.0 Documentation](#)

```
byte firstOutputSepara[] = new byte[digestLength];  
for(int i=0; i<digestLength; i++){  
    firstOutputSepara[i] = inputSepara[i];  
}  
int finalLength = input.length - digestLength;  
byte secondOutputSepara[] = new byte[finalLength];  
int i = digestLength;
```

run | save results | view score

Bob

encoding UTF-8

output

Confronto hash: true

Man Lo sono io!

Save

Run

Piattaforma AlmaChannel

- Piattaforma di e-learning d'Ateneo
- Supporto alla didattica attraverso:
 - strumenti di comunicazione
 - sincrona (chat)
 - asincrona (forum, FAQ, annunci)
 - aree di scambio e condivisione risorse
 - area pubblica
 - area privata
 - area elaborati (visibile all'utente e ai docenti o ai tutor)
 - aree per la pubblicazione di materiali didattici e risorse aggiuntive (ad es. laboratori)
 - test di autovalutazione
 - ...

Istanza del corso su AlmaChannel

- URL:
 - <http://servera.almachannel.unibo.it/sicurezza>
- Login
 - Personale:
 - Username / password possono essere richiesti a lezione o via mail (anna.riccioni@gmail.com)
 - Anonimo:
 - Username = **visitatore**
 - Password = **visitatore**

AlmaChannel: login

The screenshot shows the login page of AlmaChannel. The browser title is "AlmaChannel - Autenticazione - Mozilla Firefox". The address bar shows the URL: <https://servera.almachannel.unibo.it/sicurezza/handlers/almachannel/components/LoginPage.viewDefault>. The page features the AlmaChannel logo and the Alma Mater Studiorum University of Bologna logo. Below the logos, there is a banner for "TECNOLOGIE PER LA SICUREZZA L-5" with a description: "Questo corso è orientato a dare agli studenti una preparazione di base che consenta di progettare, utilizzare e gestire meccanismi e servizi atti a fronteggiare attacchi intenzionali all'integrità, alla riservatezza ed alla disponibilità dell'informazione." The main content area is divided into four sections: "accedi alla piattaforma" (login form with fields for username, password, and a "password dimenticata?" link, and a "login" button), "Obiettivi" (listing concepts like algorithms and protocols), "Struttura" (describing the course as an 8-week module), and "Calendario" (stating the course runs from January 23 to March 18, 2006). The footer includes "Versione 1.1" and "servera.almachannel.unibo.it".

AlmaChannel: scrivania

The screenshot shows the desktop interface of AlmaChannel. The browser title is "AlmaChannel - Scrivania - Mozilla Firefox". The address bar shows the URL: <https://servera.almachannel.unibo.it/sicurezza/handlers/almachannel/components/MyDeskPage.viewDefault>. The page features the AlmaChannel logo and the Alma Mater Studiorum University of Bologna logo. Below the logos, there is a navigation menu with links for "scrivania", "mappa", "tutors", "help", and "logout". The main content area is divided into several sections: "Benvenuto visitatore" (welcome message), "Materiale corso" (course materials), "registri studenti" (student records), "Area documenti" (document area), "Annunci" (announcements), "Forum" (forum), "Chat" (chat), and "Esercizi" (exercises). The "annunci" section contains a notice about course registration and lessons. The "forum" section contains a notice about the use of the platform and problems/queries. The "chat" section shows "Nessuna stanza trovata". The footer includes "© copyright 2004 AlmaChannel realizzato da Citam" and "servera.almachannel.unibo.it".

AlmaChannel: moduli didattici

The screenshot shows the AlmaChannel website in Microsoft Internet Explorer. The browser's address bar displays the URL: https://servera.almachannel.unibo.it/sicurezza/handlers/almachannel/components/CourseContentPage.viewDefault?_p._p.handlerName=default&_p.handlerName=default&htmlContent=-. The website header includes the AlmaChannel logo, the Alma Mater Studiorum University of Bologna logo, and navigation links: scrivania, mappa, tutors, help, logout. The main content area is titled 'Moduli didattici' and includes a sidebar with a navigation menu: Materiale corso (with sub-items: descrizione, programma, staff, calendario, moduli didattici, link, faq), Registro studenti, Area documenti, Annunci, Forum, Chat, Esercizi, and Amministrazione. The main content area features sections for 'Laboratori virtuali' and 'Approfondimenti'. The 'Laboratori virtuali' section contains text about accessing laboratory resources. The 'Approfondimenti' section contains text about a page with related topics. A 'vai a: Gestione contenuti' dropdown menu is visible. The footer includes copyright information: © copyright 2004. AlmaChannel realizzato da Citam.

AlmaChannel: forum

The screenshot shows the AlmaChannel website in Mozilla Firefox. The browser's address bar displays the URL: https://servera.almachannel.unibo.it/sicurezza/handlers/forum/components/ForumBoardPage.viewDefault?_p.handlerName. The website header is identical to the previous screenshot. The main content area is titled 'Forum' and includes a sidebar with the same navigation menu as above. The main content area features a search bar labeled 'cerca nelle discussioni' with 'cerca' and 'annulla' buttons. Below the search bar, there are two forum sections: 'Generale - Forum legati alla piattaforma AlmaChannel' and 'Corso - Forum legati al 'Corso \$XXXX\$''. Each section lists a topic, 'Problemi e giudizi', and shows '1 discussione/i | 0 risposta/e | Nessuna risposta'. The footer includes copyright information: © copyright 2004. AlmaChannel realizzato da Citam.

AlmaChannel: aree documenti

AlmaChannel - Area documenti - Mozilla Firefox

File Modifica Visualizza Vai Segnalibri Strumenti ?

https://servera.almachannel.unibo.it/sicurezza/handlers/documentarea/components/DocumentAreaPage.viewDefault?_p... Vai

Come iniziare Ultime notizie Mozilla Italia Forum di aiuto

ALMA CHANNEL
LA PIATTAFORMA DI e-LEARNING DELL'ATENEO

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

scrivania mappa tutors help logout

Area documenti
Ritorna a: scrivania

- Materiale corso
 - descrizione
 - programma
 - staff
 - calendario
 - moduli didattici
 - link
 - faq
- Registro studenti
- Area documenti
- Annunci
- Forum
- Chat
- Esercizi

utente: visitatore

copyright 2004. AlmaChannel
realizzato da Citam

Completato servera.almachannel.unibo.it

AlmaChannel: documenti condivisi

AlmaChannel - Scambio - Mozilla Firefox

File Modifica Visualizza Vai Segnalibri Strumenti ?

https://servera.almachannel.unibo.it/sicurezza/handlers/documentarea/components/FolderPage.viewDefault?_p... Vai

Come iniziare Ultime notizie Mozilla Italia Forum di aiuto

ALMA CHANNEL
LA PIATTAFORMA DI e-LEARNING DELL'ATENEO

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

scrivania mappa tutors help logout

Scambio
Ritorna a: scrivania :: area documenti

nuovo

| Tipo | Nome | Autore | Pubblicazione | Dim. (KB) | apri | scarica | elimina |
|------|---|---------------|---------------|-----------|------|---------|---------|
| | comp_FIPS_140-2_and_140-1 | Riccioni Anna | 06/02/06 | 274 | | | |
| | FIPS_140_2 | Riccioni Anna | 06/02/06 | 1,432 | | | |

documenti totali: 2
pagina 1 di 1

copyright 2004. AlmaChannel
realizzato da Citam

Completato servera.almachannel.unibo.it