Jasypt
Java Simplified Encryption

Laboratorio di Reti
2014/2015
Prof. Laura Ricci

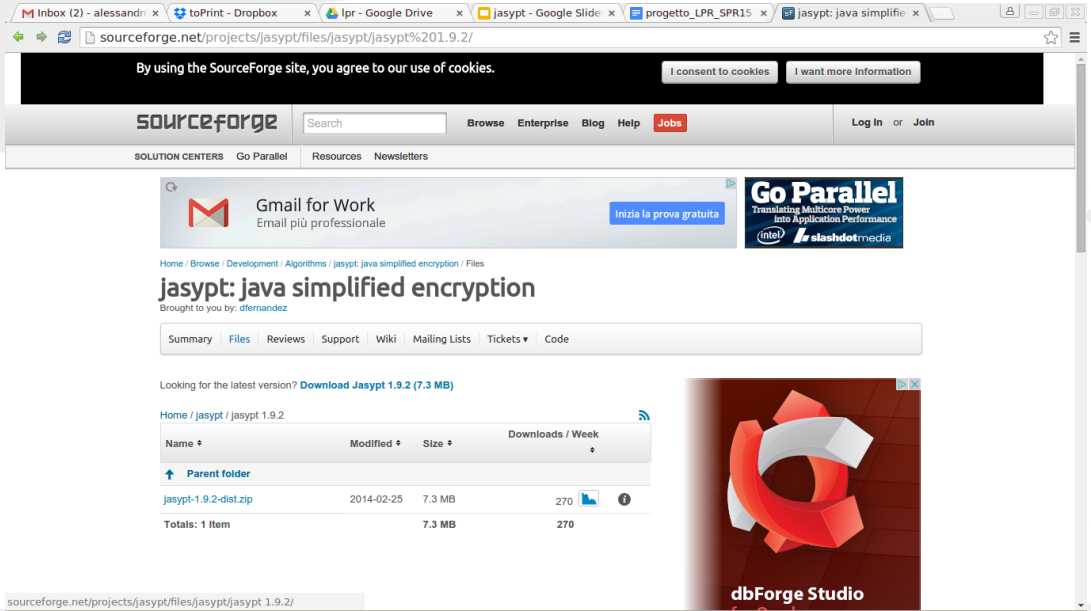
Speaker: Alessandro Lulli - lulli@di.unipi.it

Jasypt

- una libreria per fare encrypting / decrypting in Java

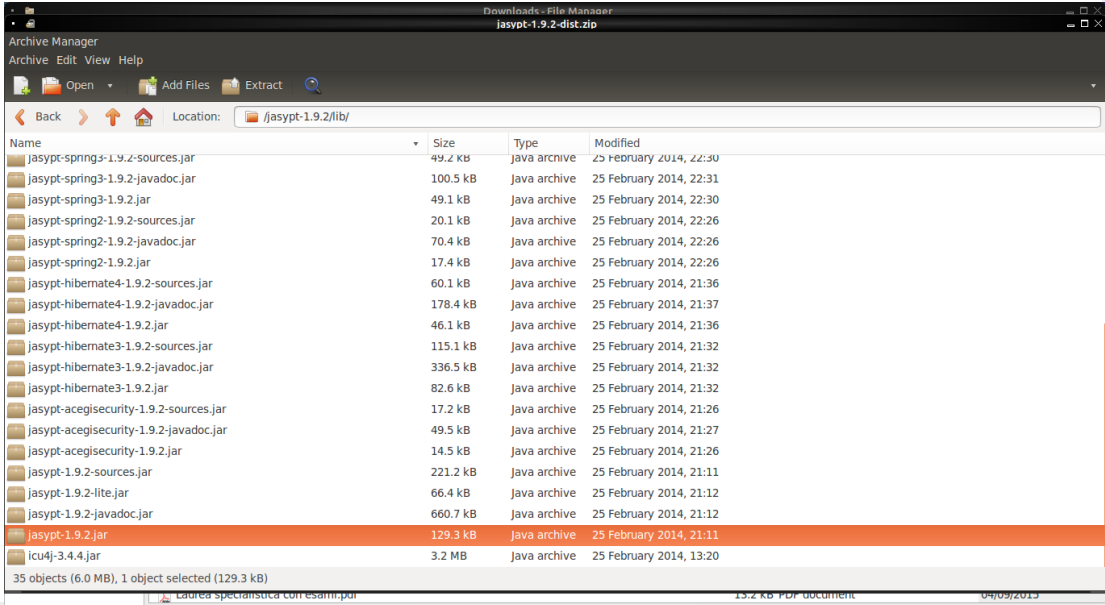
Download

- Jasypt può essere scaricato dal seguente link:
  - http://www.jasypt.org/index.html
- i test sono stati fatti con jasypt 1.9.2



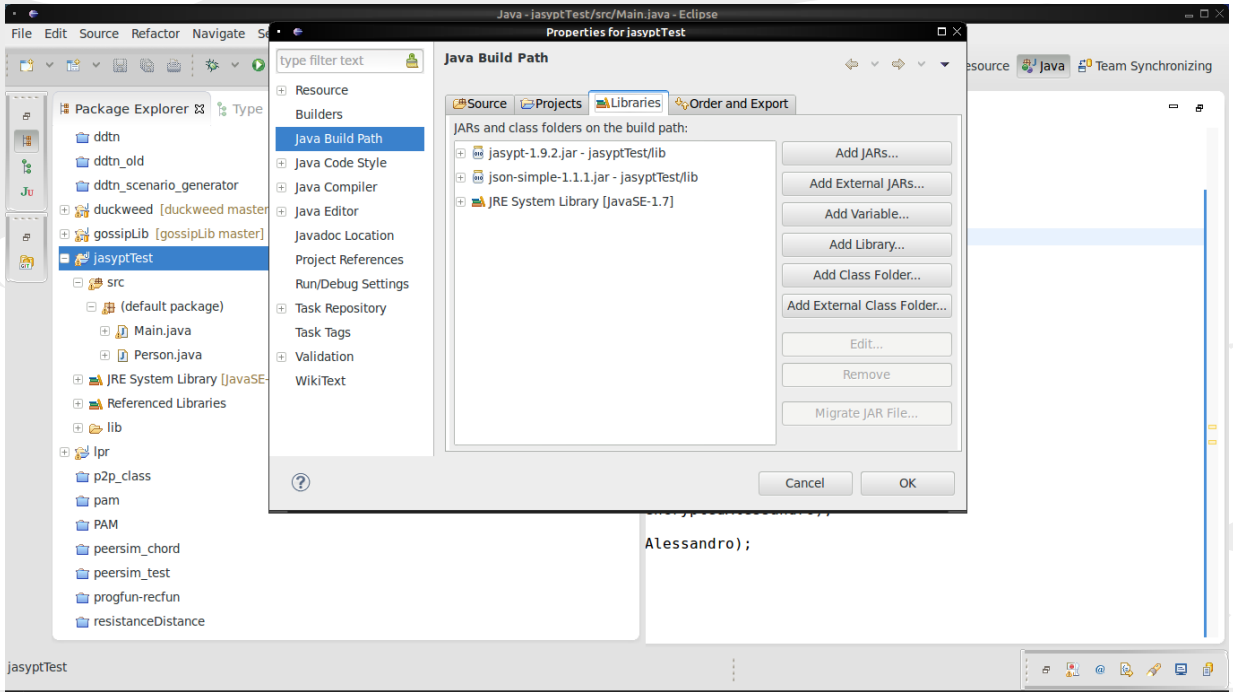
Install in Eclipse (I)

- decomprimere lo script ed estrarre la libreria *jasypt-1.9.2.jar* nella folder del progetto Eclipse
- il file è nella seguente cartella:
  - /jasypt-1.9.2/lib/



Install in Eclipse (II)

- aggiungere la libreria jasypt-1.9.2.jar



Encrypt / Decrypt di testo (I)

- si crea una password di tipo String
- la password dovrà essere condivisa tra chi esegue la encrypt e chi esegue il decrypt

```
import org.jasypt.util.text.BasicTextEncryptor;


public class Main
{

    public static void main(final String[] args)
    {
        final String password = "strongPassword";

        final BasicTextEncryptor encryptor = new BasicTextEncryptor();
        encryptor.setPassword(password);

        final String encryptedString = encryptor.encrypt("Parola segreta");

        System.out.println("Encrypted String: "+encryptedString);

        final String decryptedString = encryptor.decrypt(encryptedString);

        System.out.println("Decrypted String: "+decryptedString);
```

Encrypt / Decrypt di testo (II)

- si crea una classe di tipo *BasicTextEncryptor*
  - sarà il nostro encryptor / decryptor di stringhe
- si setta la password con il quale fare encrypt / decrypt

```
import org.jasypt.util.text.BasicTextEncryptor;


public class Main
{

    public static void main(final String[] args)
    {
        final String password = "strongPassword";

        final BasicTextEncryptor encryptor = new BasicTextEncryptor();
        encryptor.setPassword(password);

        final String encryptedString = encryptor.encrypt("Parola segreta");

        System.out.println("Encrypted String: "+encryptedString);

        final String decryptedString = encryptor.decrypt(encryptedString);

        System.out.println("Decrypted String: "+decryptedString);
```

Encrypt / Decrypt di testo (III)

- dato il nostro oggetto *encryptor*
- per encrypt: *encryptor.encrypt(“Parola segreta”);*
- per decrypt: *encryptor.decrypt(encriptedString);*

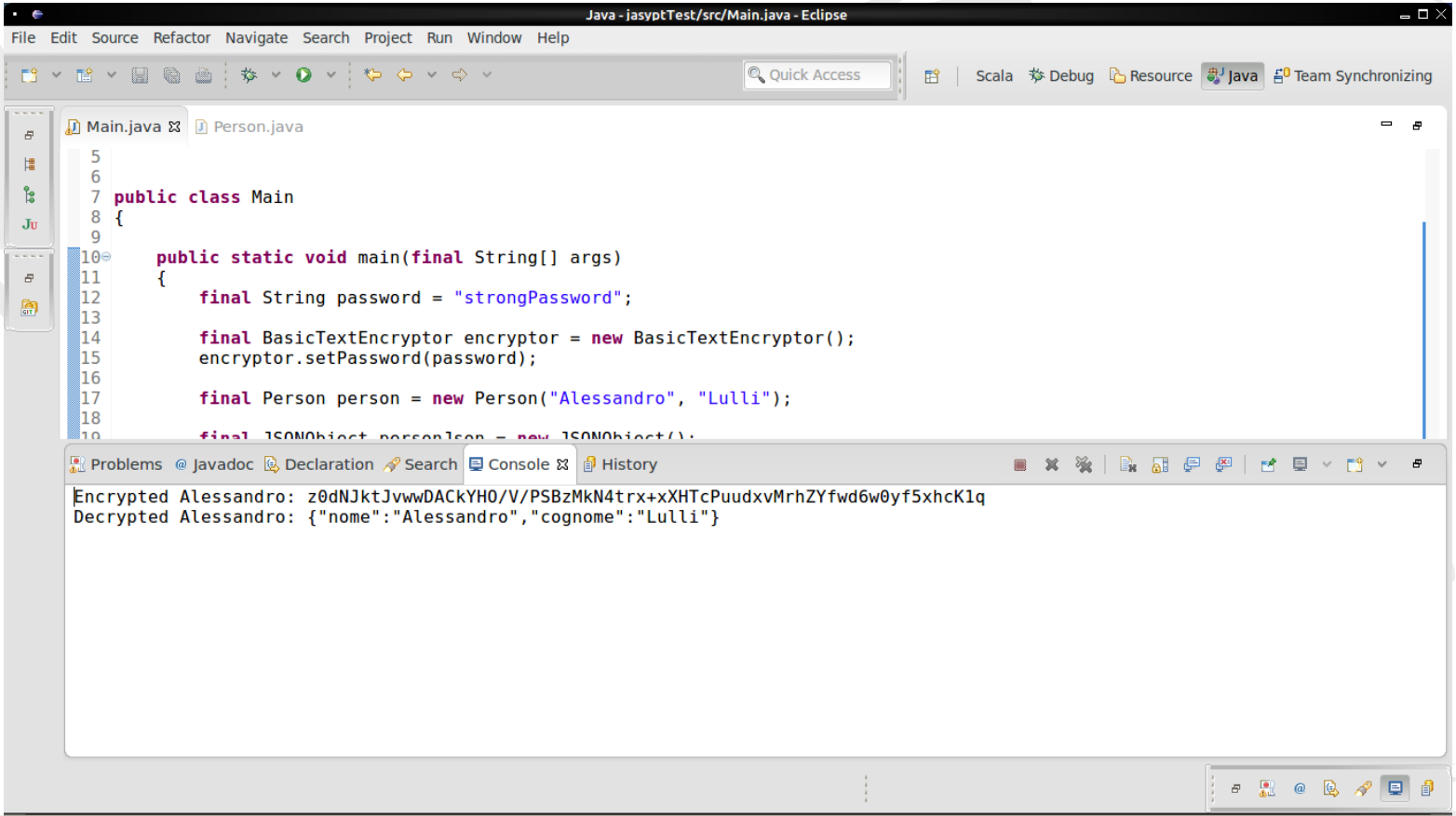
```
import org.jasypt.util.text.BasicTextEncryptor;


public class Main
{

    public static void main(final String[] args)
    {
        final String password = "strongPassword";

        final BasicTextEncryptor encryptor = new BasicTextEncryptor();
        encryptor.setPassword(password);

        final String encryptedString = encryptor.encrypt("Parola segreta");

        System.out.println("Encrypted String: "+encryptedString);

        final String decryptedString = encryptor.decrypt(encryptedString);

        System.out.println("Decrypted String: "+decryptedString);
```

Encrypt / Decrypt JSON

- si crea la string JSON e si passa alla encryptor

```
final String password = "strongPassword";

final BasicTextEncryptor encryptor = new BasicTextEncryptor();
encryptor.setPassword(password);

final Person person = new Person("Alessandro", "Lulli");

final JSONObject personJson = new JSONObject();
personJson.put("nome", person.getName());
personJson.put("cognome", person.getSurname());

final String encryptedAlessandro = encryptor.encrypt(personJson.toJSONString());

System.out.println("Encrypted Alessandro: "+encryptedAlessandro);

final String decryptedAlessandro = encryptor.decrypt(encryptedAlessandro);

System.out.println("Decrypted Alessandro: "+decryptedAlessandro);
```

Encrypt / Decrypt JSON Output



Encrypt / Decrypt Password

- si usa la classe *BasicPasswordEncryptor*
- una volta crittata la password:
  - si invia al server che farà il check con *checkPassword*