

**Criptografia e Segurança das Comunicações**

Localização Segura de Pessoas

Autores:

|  |  |
| --- | --- |
| Bruno Rosa Paixão Cardoso | 75158 |
| Rúben Miguel Oliveira Tadeia | 75268 |
| Francisco José Trigo da Cruz dos Santos Cunha | 75284 |

|  |  |  |
| --- | --- | --- |
| Grupo: | Turno: | Ano Lectivo: |
| 7 | 5ªf, 8h30 Semanas Impares | 2016-2017 |

04 de Janeiro de 2017

**1. Introdução**

Pretende-se neste trabalho desenvolver um projecto com o tema de “Localização segura de pessoas”, desenvolvendo para esse fim uma aplicação para smartphone, com o sistema operativo Android que permite localizar crianças através do uso do GPS (e/ou A-GPS) de forma privada e segura.

De forma mais pormenorizada, considerou-se ser possível a aplicação obedecer aos seguintes requerimentos:

* Envio regular de informações (encriptadas) sobre a localização do localizado para o utilizador supervisor;
* Serem tomados especiais cuidados com a forma de encriptação utilizada, de tal maneira que o localizado pode estar precisamente no mesmo local em instantes diferentes e a informação encriptada enviada, correspondente a instantes diferentes, é diferente;
* O utilizador supervisor poder pedir a localização actual do localizado;
* Permite definir alertas automáticos caso o localizado saia de um perímetro definido; Permite monitorização contínua e automática com alertas automáticos caso o sinal com o localizado se perder;
* Permite que a informação seja também enviada de modo seguro para uma base de dados num servidor, a qual está protegida, contra por exemplo SQL injection e também contra questões de privacidade “avançadas”, por exemplo, informações de autenticação de utilizadores;
* É limpo o histórico de localização na base de dados, dado que apenas se guarda a informação da última localização onde este utilizador esteve;
* Estar protegida no dispositivo do utilizador supervisor e no do localizado. Por protegido quer-se dizer que é necessária uma palavra passe para aceder à aplicação, esta informação não pode ser obtida, através de um ataque à base de dados. Isto porque, as informações de autenticação são guardadas na memória do telefone.

**2. Segurança das Comunicações**

Neste projecto, de forma a tornar a encriptação da localização mais segura foi utilizado o método de encriptação RSA. Mas antes de se explicar o seu funcionamento, convém perceber um pouco de segurança das comunicações. Antes de mais, RSA é um algoritmo de criptografia assimétrico.

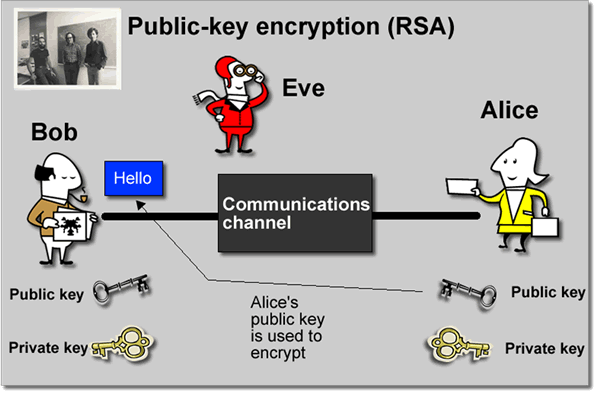


Figura 1: Funcionamento do método de encriptação RSA

A principal diferença técnica entre os algoritmos de encriptação simétricos e assimétricos é que, no caso do algoritmo assimétrico, a chave usada para encriptar uma mensagem, que não é diferente da chave usada para desencriptar. Cada utilizador tem um par de chaves, uma chave pública para encriptar e uma chave privada para desencriptar.

Em contraste, os algoritmos simétricos usam uma chave única para encriptar e desencriptar. Um algoritmo popular deste método é o AES. Esses algoritmos são geralmente mais eficientes, mas podem não ser tão seguros quanto os assimétricos.

Uma vantagem importante das encriptações assimétricas relativamente a encriptações simétricas é o facto de não ser necessário nenhum canal secreto para trocar a chave pública. O receptor apenas precisa de ter a certeza da autenticidade da chave pública. As encriptações simétricas requerem um canal secreto para enviar a chave secreta gerada noutro lado do canal de comunicação, estas requerem também uma quantidade superior de chaves.

Uma desvantagem de encriptações assimétricas sobre as encriptações simétricas é que estas tendem a ser muito mais lentas. Com isso, querer-se dizer que pode levar cerca de 1000 vezes mais tempo de CPU para processar uma encriptação/desencriptação assimétrica do que uma criptografia encriptação/desencriptação simétrica.

Outra desvantagem é que as cifras simétricas podem facilmente ser alvo de um ataque de "força bruta", no qual todas as chaves possíveis são tentadas até que a chave correta seja encontrada.

**3. Especificação do Algoritmo Implementado**

A nossa aplicação utiliza o seguinte fluxograma abaixo.

Fluxograma.png

Figura 2: Fluxograma da Aplicação Android

Foi também criado para a aplicação um nome “SecLoc” de Secure Location, assim como o seu respectivo logotipo.



Figura 3: Icon da aplicação SecLoc

**4. Implementação**

**4.1. Classe Main**



Figura 4: Código para a classe Main parte 1

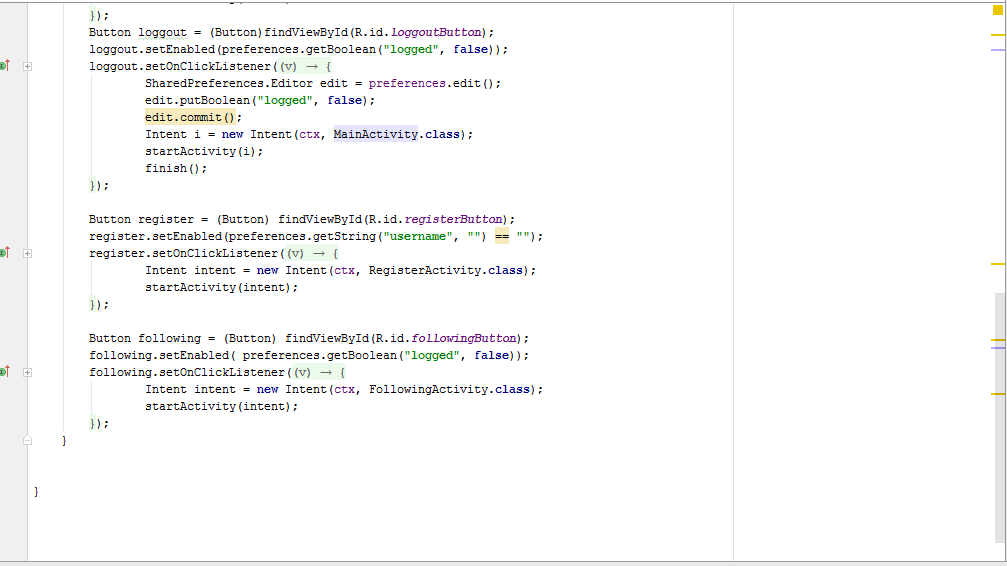


Figura 5: Código para a classe Main parte 2

**4.2. Classe Register**

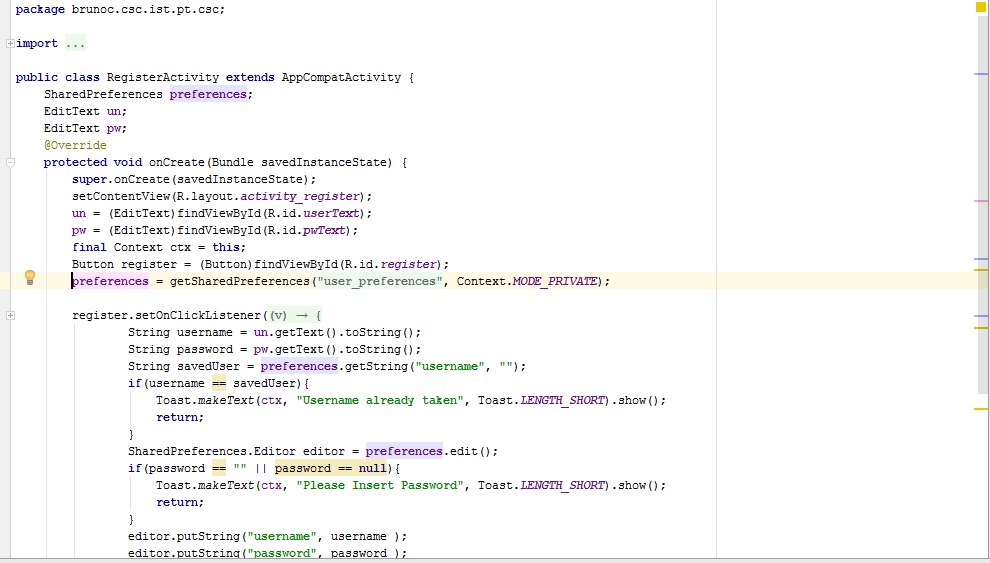


Figura 6: Código para a classe Register parte 1

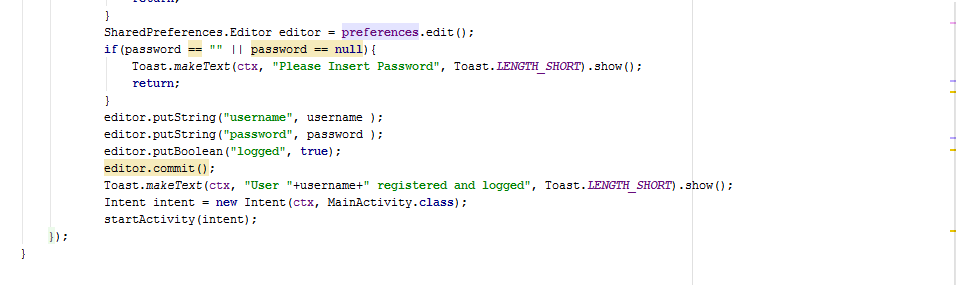


Figura 7: Código para a classe Register parte 2

**4.3. Classe Login**



Figura 8: Código para a classe Login parte 1



Figura 9: Código para a classe Login parte 2

**4.4. Classe Following**

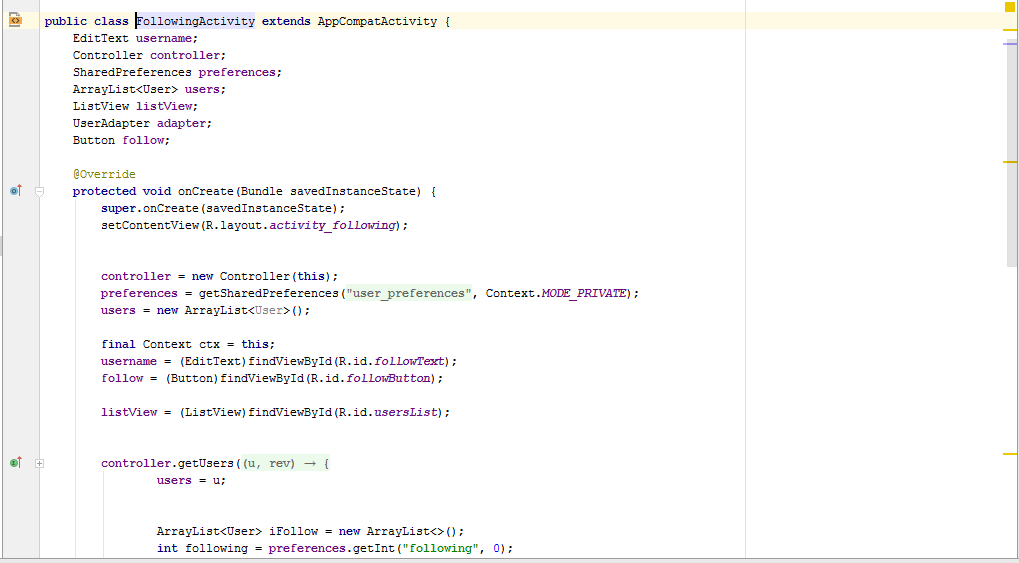


Figura 10: Código para a classe Following parte 1

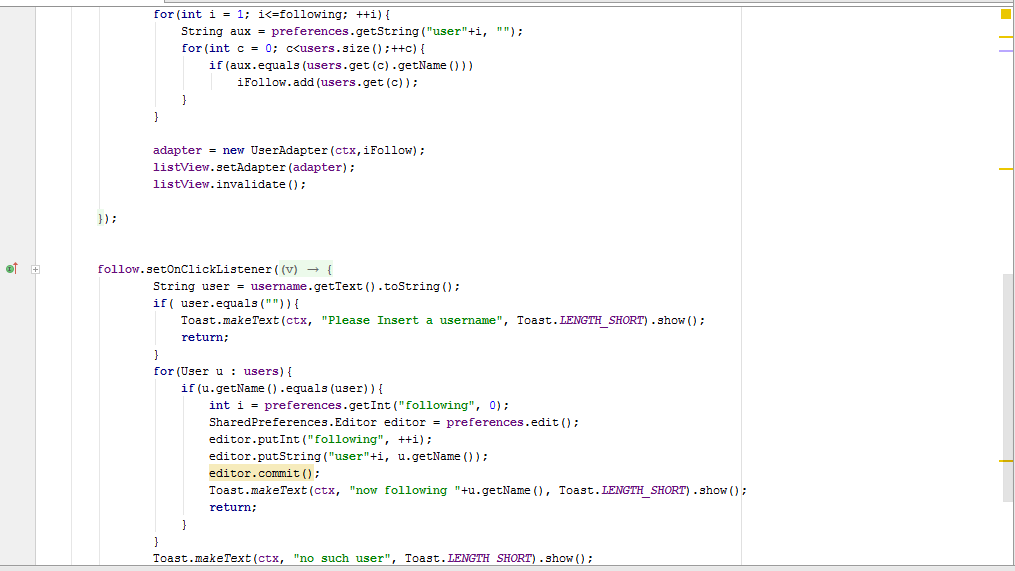


Figura 11: Código para a classe Following parte 2

**4.5. Classe Locator**

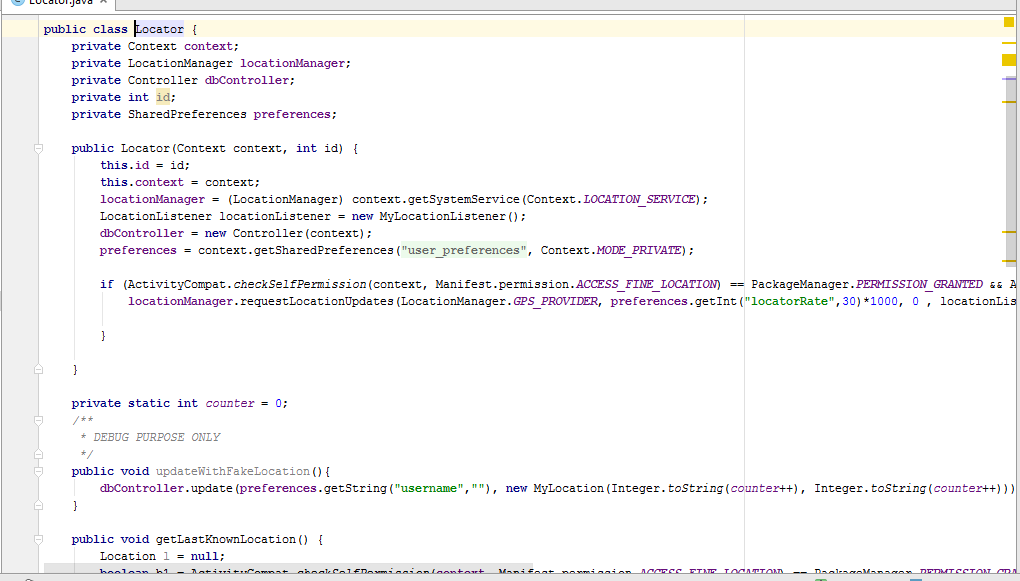


Figura 12: Código para a classe Locator parte 1



Figura 13: Código para a classe Locator parte 2

**4.6. Classe Preferences**

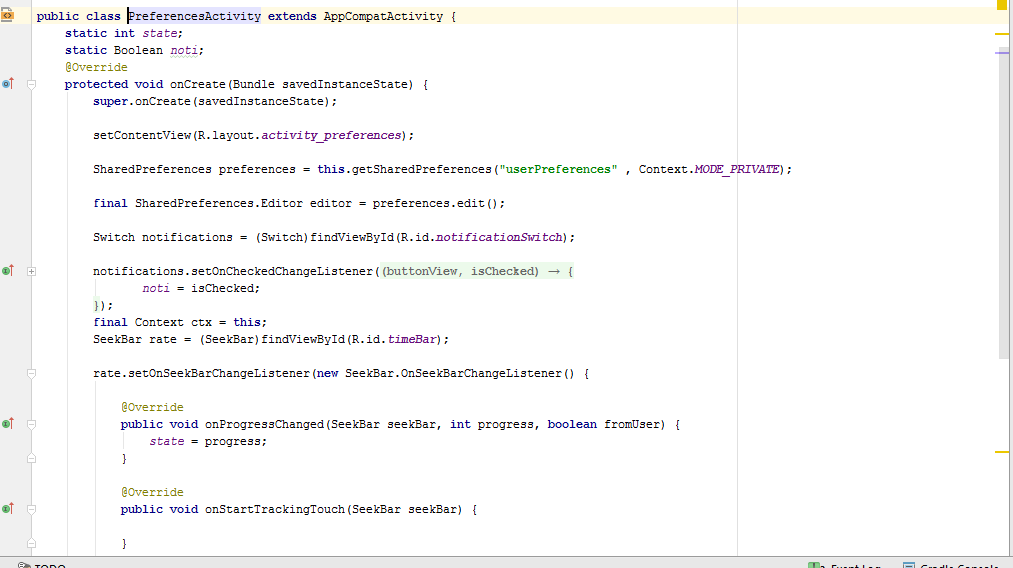


Figura 14: Código para a classe Preferences parte 1



Figura 15: Código para a classe Preferences parte 2

**4.7. Classe Encryptor**

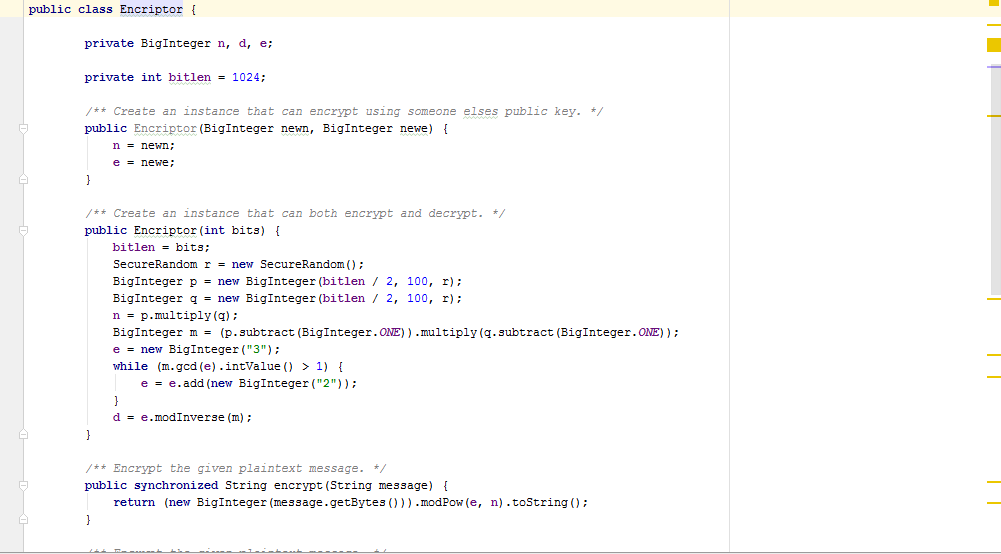


Figura 16: Código para a classe Encryptor parte 1

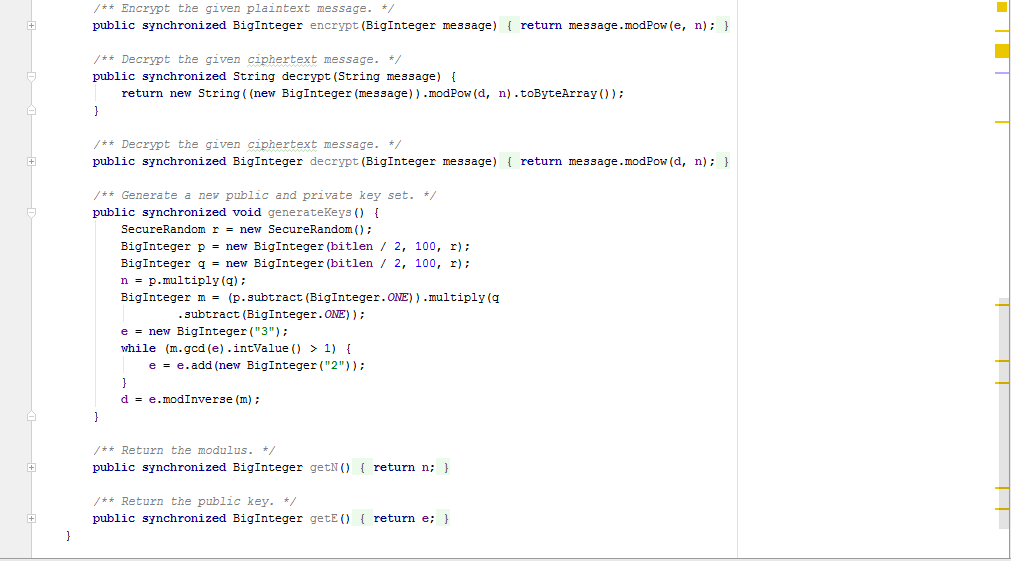


Figura 17: Código para a classe Encryptor parte 2

**4.8. Classes User, User Adapter e My Location**

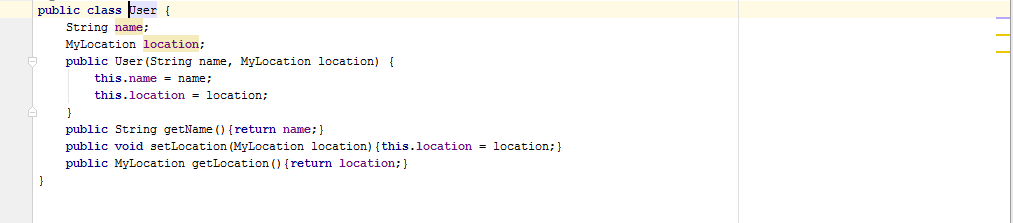


Figura 18: Código para a classe User

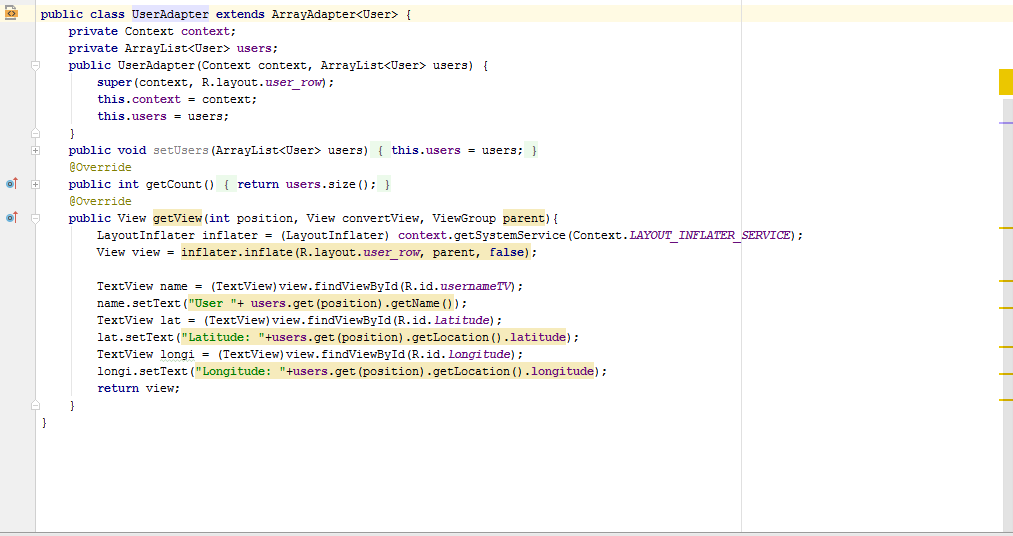


Figura 19: Código para a classe User Adapter

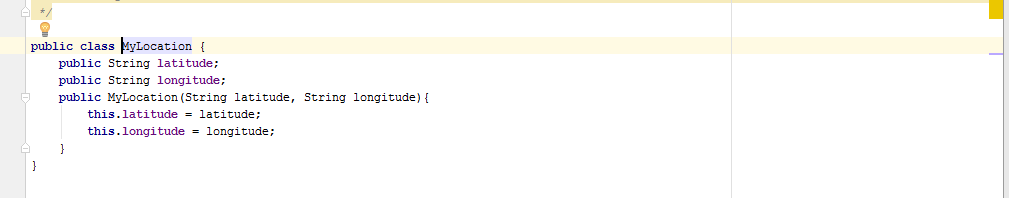


Figura 20: Código para a classe MyLocation

**4.9 Classes Controller e Cloudant Controller**

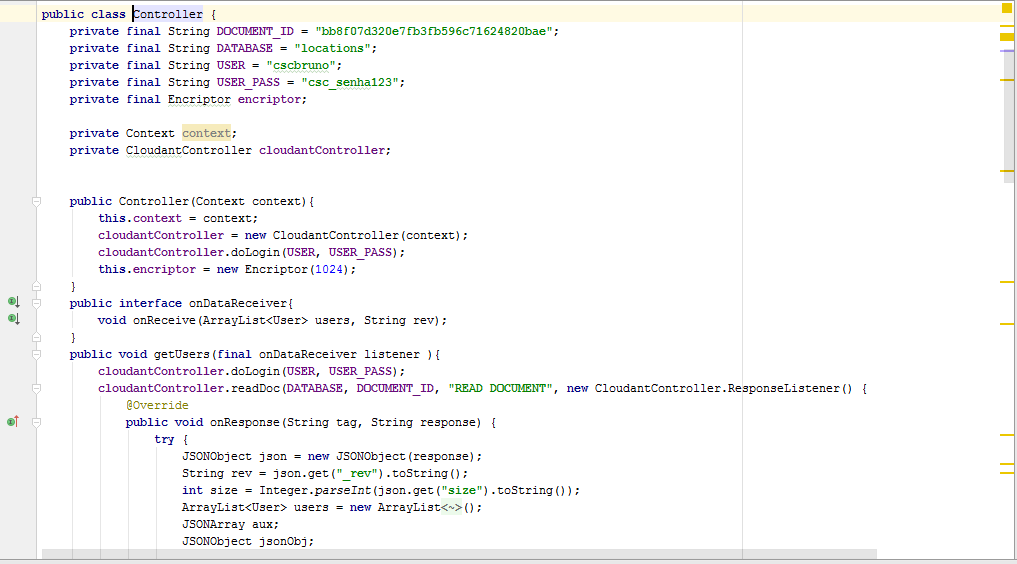


Figura 21: Código para a classe Cloudant Controller

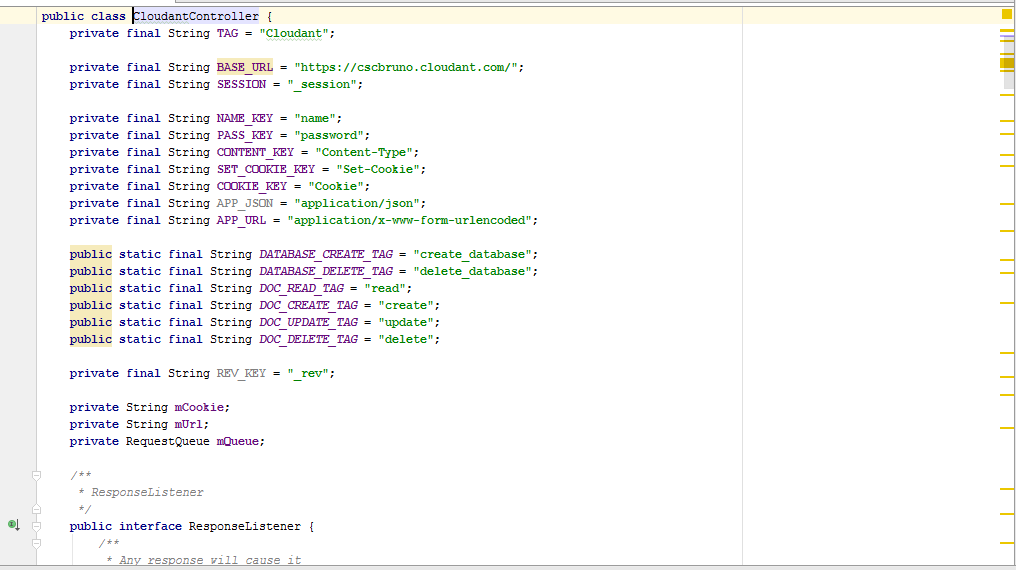


Figura 22: Código para a classe Controller

**5. Testes e Resultados**

Para testar a aplicação, foi feito um teste com a mesma em dois smartphones distintos sendo um o possível pai e o outro o possível filho, apesar de a aplicação ser idêntica e de ter todas as funcionalidades disponíveis em ambos os casos. Foi feito um “follow” de um utilizador por parte do outro e a localização foi recebida corretamente, como esperado em latitude e longitude, e de seguida foi feita a verificação da localização utilizando o Google Maps onde se constatou que a localização estava correta. No entanto na base de dados online Cloudant (que é uma base de dados online NoSQL, promovida pela IBM) nenhuma destas localizações é identificável devido a estarem encriptadas.

O processo relativo à aplicação foi gravado num vídeo ilustrativo terá utilidade na apresentação, comprovando assim o funcionamento da app.

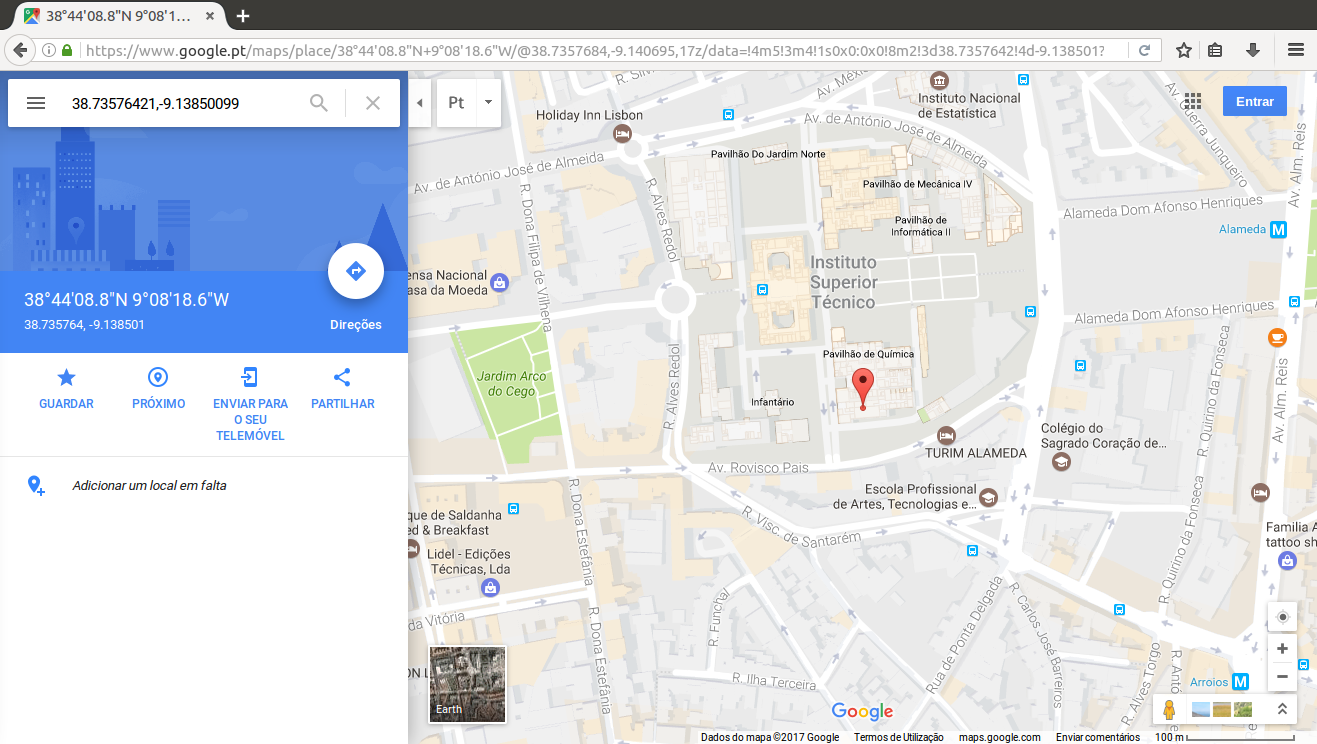


Figura 23: Resultado do Google Maps face às coordenadas recebidas

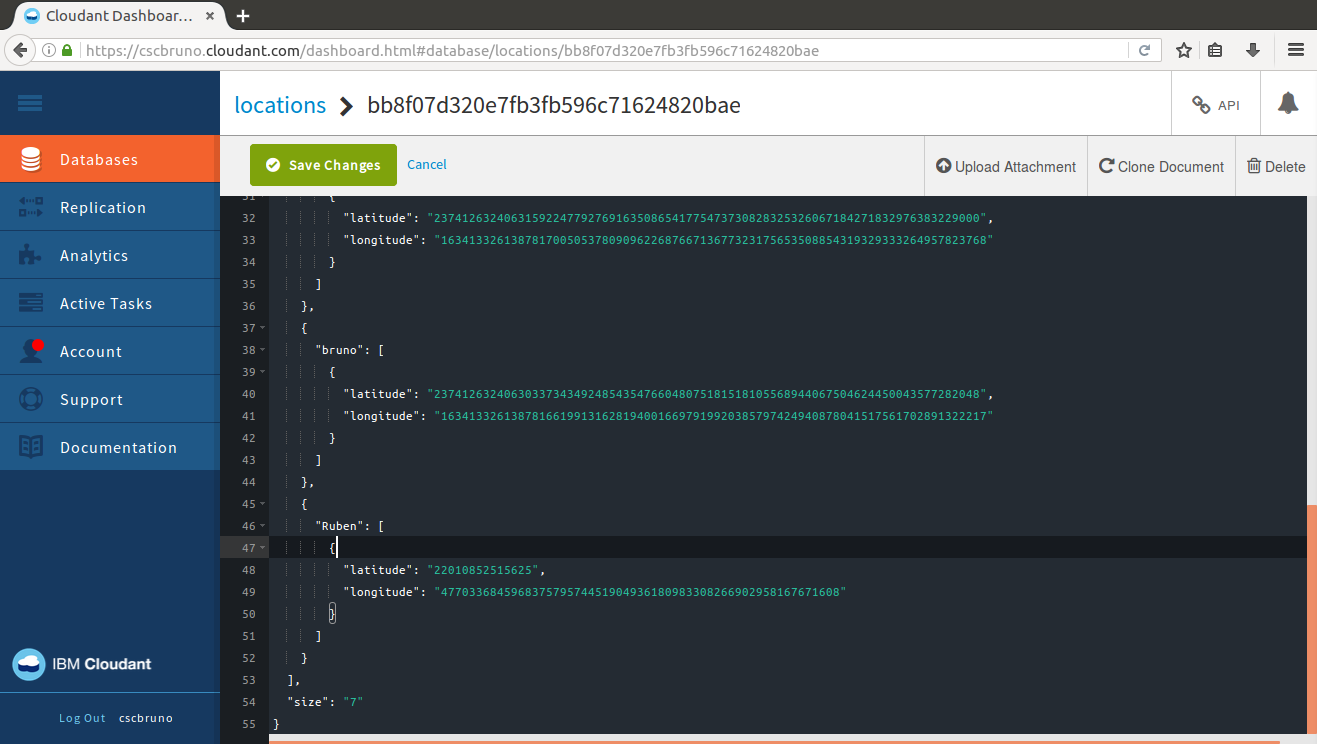


Figura 24: Conteúdo da Base de dados após o teste da aplicação

**6. Referências**

* [**Figura 1 - http://d2o0t5hpnwv4c1.cloudfront.net/1115\_apiWebApp/images/rsa.gif**](http://d2o0t5hpnwv4c1.cloudfront.net/1115_apiWebApp/images/rsa.gif)
* [**Código - http://www.developer.com/ws/android/encrypting-with-android-cryptography-api.html**](http://www.developer.com/ws/android/encrypting-with-android-cryptography-api.html)
* [**RSA Funcionamento - http://doctrina.org/How-RSA-Works-With-Examples.html**](http://doctrina.org/How-RSA-Works-With-Examples.html)
* [**RSA - http://doctrina.org/Why-RSA-Works-Three-Fundamental-Questions-Answered.html**](http://doctrina.org/Why-RSA-Works-Three-Fundamental-Questions-Answered.html)