



Localização segura de pessoas

Instituto Superior Técnico
Universidade de Lisboa, Portugal



Bruno Cardoso, n° 75158
Francisco Cunha, n° 75284
Rúben Tadeia, n° 75268



1. INTRODUÇÃO



Introdução

- Hoje em dia são utilizados trackers em veículos de transportes;
- Nos Estados Unidos foi criada legislação para a participação voluntária de crianças com autismo e outras perturbações num programa de tracking GPS;
- Porque não usar a potencialidade GPS de inúmeros smartphones?



2. OBJETIVOS



Objetivos

- Criação de uma aplicação para localização segura de pessoas:
 - A aplicação deve enviar regularmente informações de localização encriptadas;
 - O sistema deve ter no mínimo dois utilizadores, o que requiere a localização e o localizado;
 - O localizador deve poder pedir a localização do localizado (sem esperar pelo próximo envio).



3. IMPLEMENTAÇÃO



Implementação (1)





Implementação (2)

- A aplicação é desenvolvida para Android;
- Os telefones comunicam usando a arquitectura da Internet com uma base de dados a mediar o processo;
- A localização é obtida exclusivamente usando o Sistema GPS;
- Cada utilizador tem associado a si um username e uma password;



Implementação (3)

- A aplicação permite o registo na base de dados;
- A aplicação permite a leitura da localização de um utilizador registado, desde que saiba o seu nome;
- A base de dados responde com a última localização registada;
- A aplicação permite o envio automático da localização do localizado;

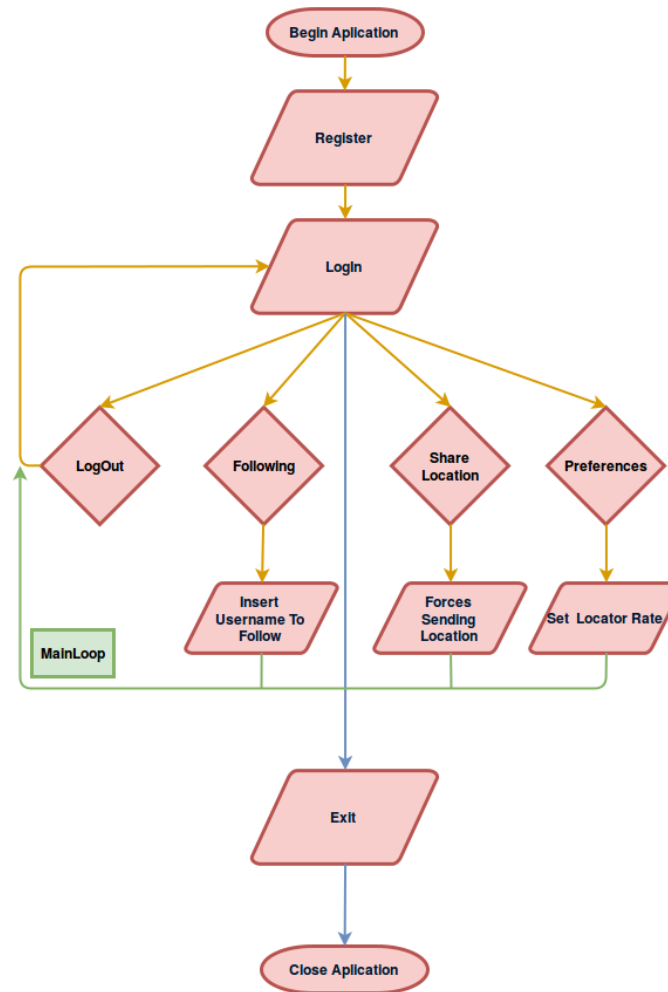


Implementação (4)

- O utilizador escolhe a frequência de envio de informações para a base de dados – entre 1 e 30 min, default é 1 minute;
- O utilizador pode forçar o envio da sua localização de forma manual (opção “share”);
- Um utilizador não registado não pode seguir (saber a localização) de outras pessoas.
- A comunicação com a base de dados usa JSON, e a base de dados está alojada pela CSC Cloudant.



Implementação (5)





3. SEGURANÇA NAS COMUNICAÇÕES

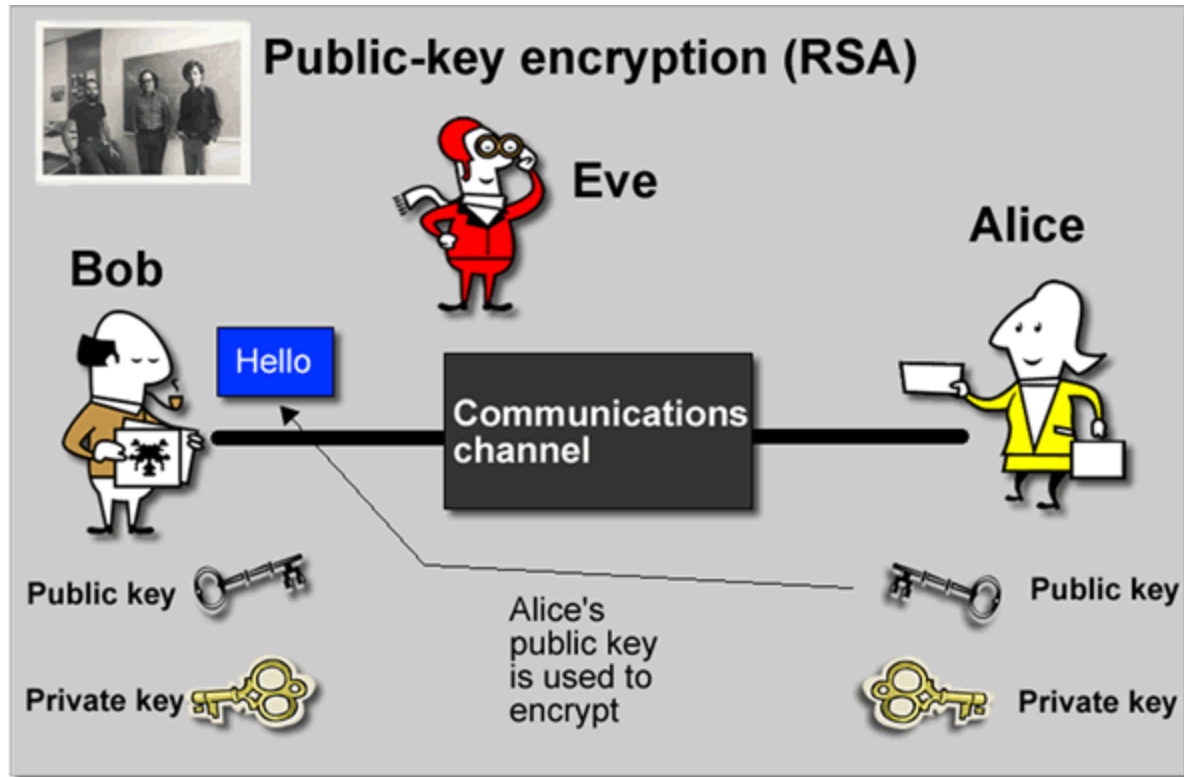


Segurança nas comunicações (1)

- A comunicação entre o utilizador e a base de dados é feita de tal forma que os dados enviados e recebidos estão encriptados;
- A informação relativa à localização dos utilizadores na base de dados, está, pois, encriptada;
- É usado o protocolo RSA nas comunicações, para as tornar seguras;



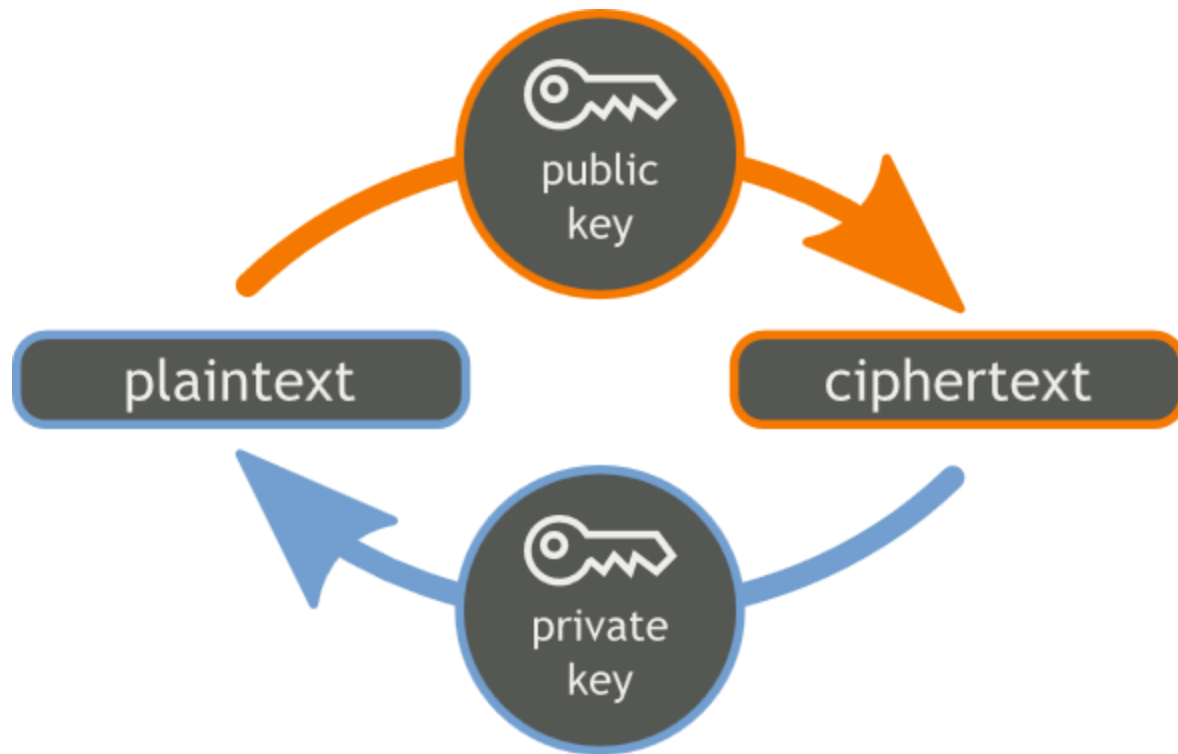
Segurança nas comunicações (2)



Source: [www.amfastech.com]



Segurança nas comunicações (3)



Source: [<https://www.linkedin.com/pulse/>]

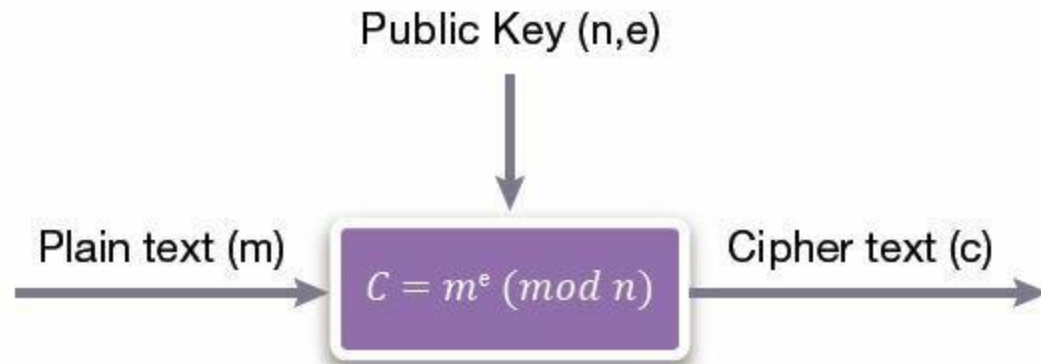


Segurança nas comunicações (4)

- P e q primos;
- $n = p \times q$;
- $\phi(n) = (p-1) \cdot (q-1)$;
- Escolher um inteiro e tal que $1 < e < \phi(n)$, de forma que e e $\phi(n)$ sejam primos entre si.
- Calcular d tal que $de \equiv 1 \pmod{\phi(n)}$;



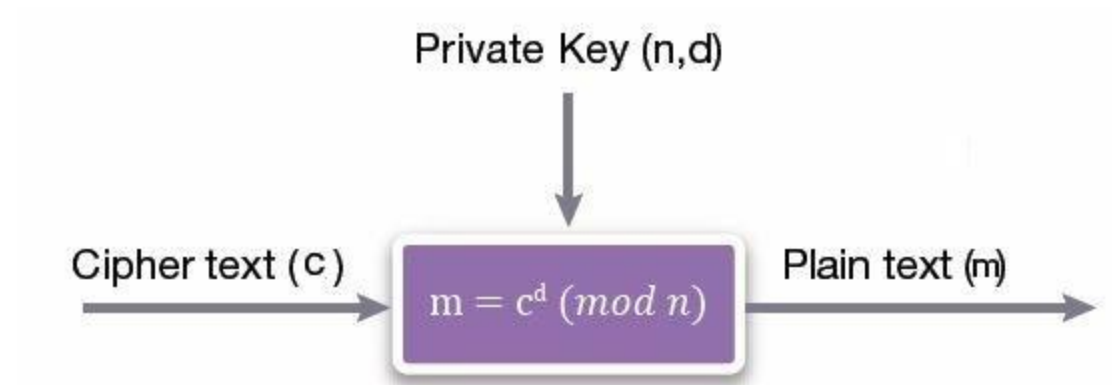
Segurança nas comunicações (5)



Source: [<https://www.linkedin.com/pulse/>]



Segurança nas comunicações (6)



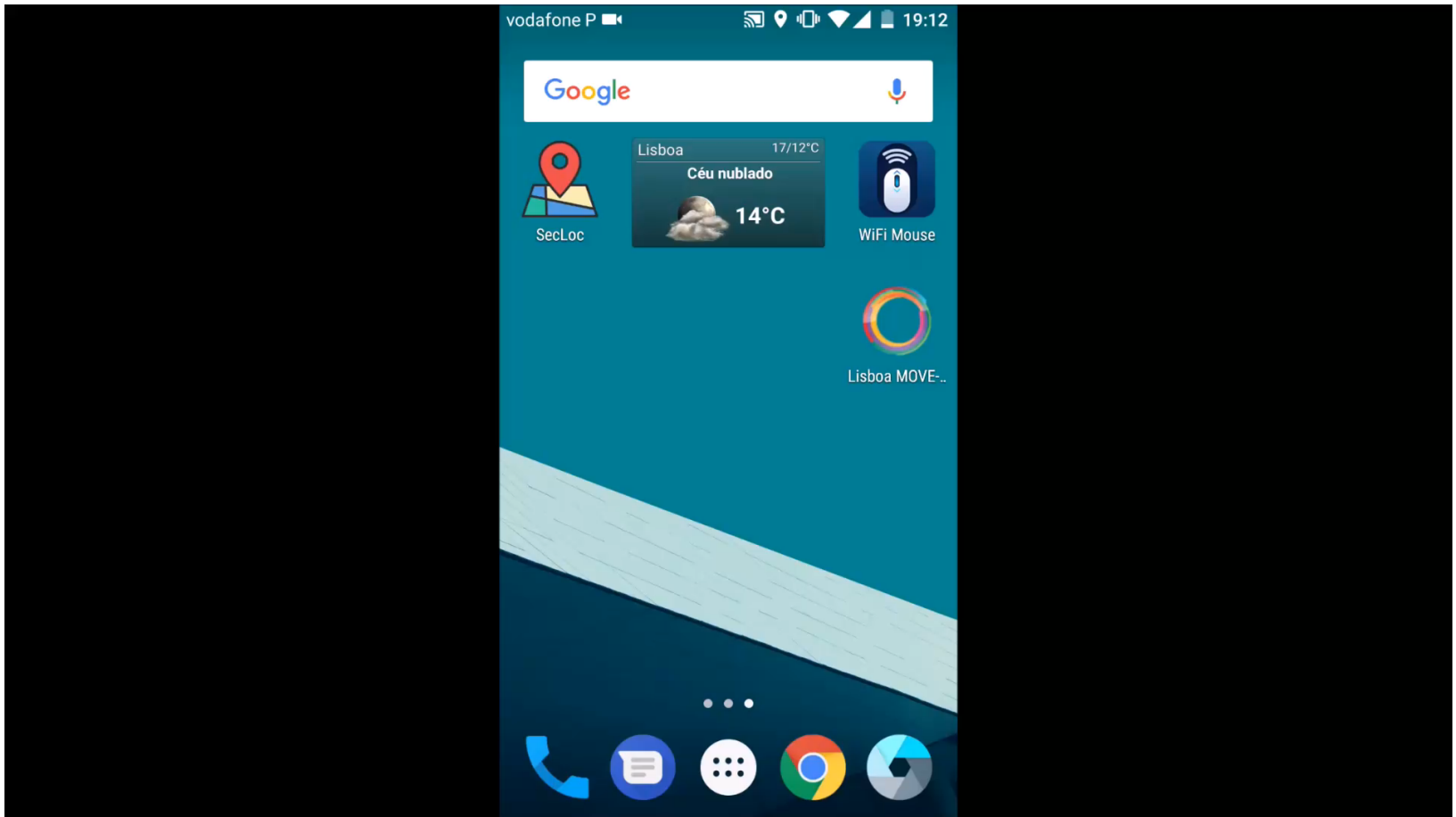
Source: [<https://www.linkedin.com/pulse/>]



5. TESTE



Teste no lado do localizado





Informação na base de dados

Cloudant Dashboard... x +

https://cscbruno.cloudant.com/dashboard.html#database/locations/bb8f07d320e7fb3fb596c71624820bae

locations > bb8f07d320e7fb3fb596c71624820bae

API

Save Changes Cancel Upload Attachment Clone Document Delete

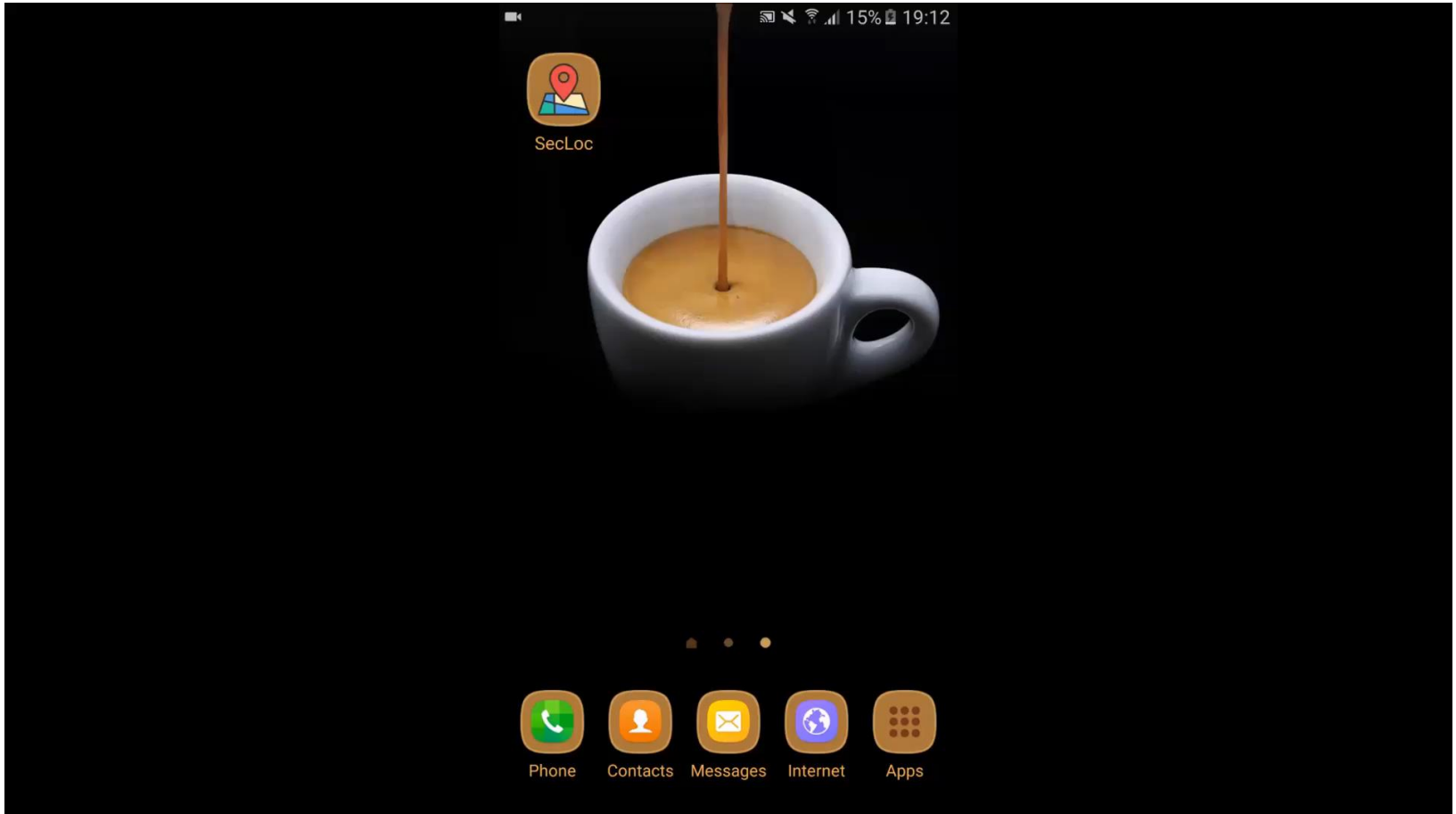
```
31 | | | | {
32 | | | |   "latitude": "237412632406315922477927691635086541775473730828325326067184271832976383229000",
33 | | | |   "longitude": "163413326138781700505378090962268766713677323175653508854319329333264957823768"
34 | | | | }
35 | | | | ]
36 | | | | },
37 | | | | {
38 | | | |   "bruno": [
39 | | | |     {
40 | | | |       "latitude": "237412632406303373434924854354766048075181518105568944067504624450043577282048",
41 | | | |       "longitude": "163413326138781661991316281940016697919920385797424940878041517561702891322217"
42 | | | |     }
43 | | | |   ]
44 | | | | },
45 | | | | {
46 | | | |   "Ruben": [
47 | | | |     {
48 | | | |       "latitude": "22010852515625",
49 | | | |       "longitude": "477033684596837579574451904936180983308266902958167671608"
50 | | | |     }
51 | | | |   ]
52 | | | | }
53 | | | | ],
54 | | | | "size": "7"
55 | | | | }
```

IBM Cloudant

Log Out cscbruno

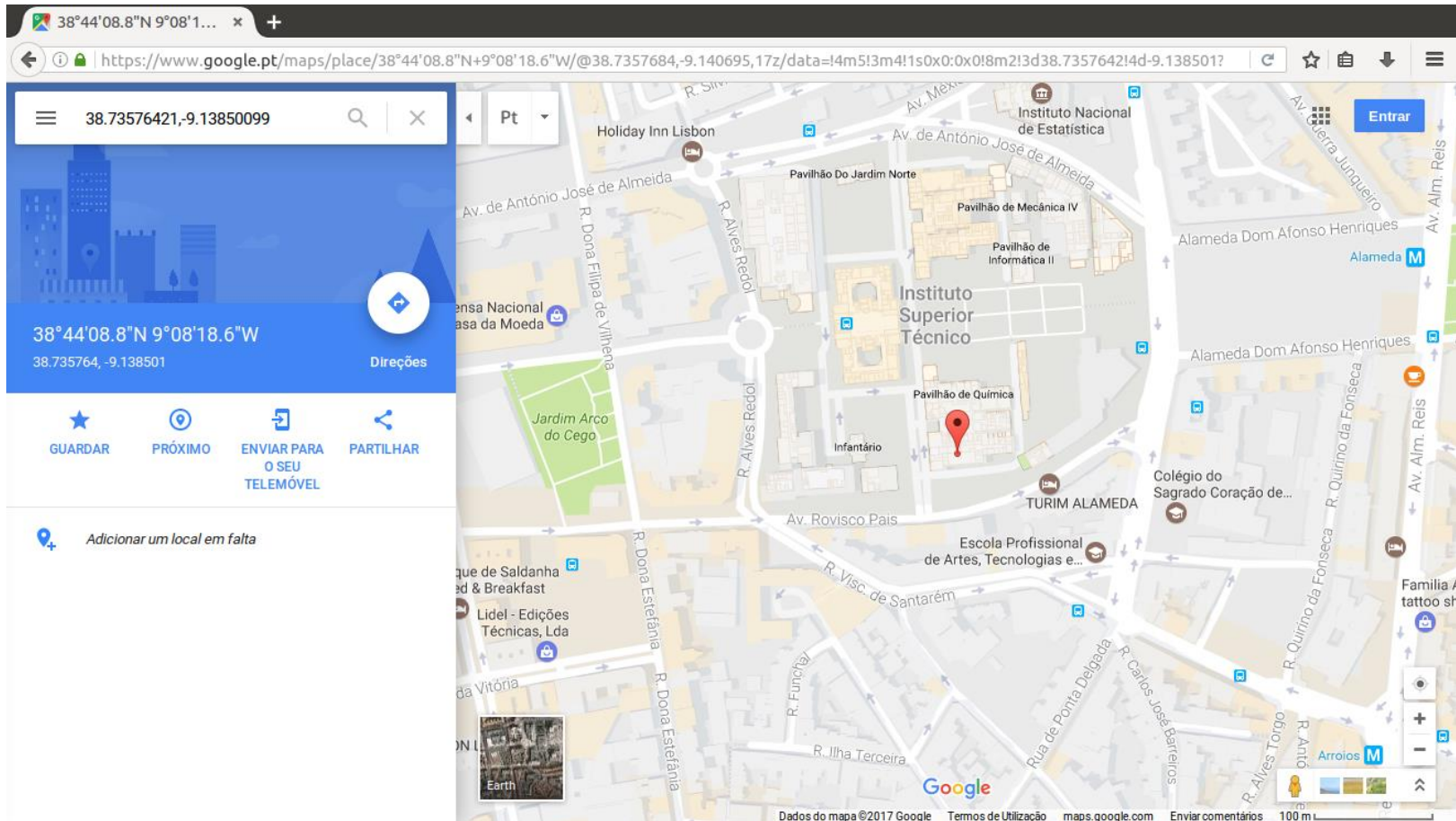


Teste no lado do localizador





Coordenadas recebidas





6. REFERÊNCIAS



Referências

- <https://www.nytimes.com/2014/01/30/nyregion/us-will-finance-devices-to-track-children-with-autism.html>;
- <http://www.amfastech.com/2013/04/the-rsa-encryption-algorithm-explained.html>;
- <https://www.linkedin.com/pulse/rsa-encryption-explained-maaz-shah>;
- <https://pt.wikipedia.org/wiki/RSA>.