|  |
| --- |
| 哈尔滨工业大学(深圳) |
| **《网络与系统安全》 实验报告** |
|  |
| 实验四  PKI 实验  学 院:   |  |  | | --- | --- | | 姓 名: |  | | 学 号: |  | | 专 业: |  | | 日 期: | 2023年4月 | |

1. 根据如下命令查看证书信息，并回答下面两个问题。

命令为：openssl x509 -in ca.crt -text -noout。

1. 证书的哪部分内容表明这是证书的持有方？

（2）从证书的哪部分内容可以看出这是自签名的证书？

1. 用如下命令查看[www.bank32.com](http://www.bank32.com)的服务器证书，至少说出与ca.crt的证书的两点不同。

openssl x509 -in server.crt -text -noout：

1. 请将能够正确访问www.bank32.com的截图贴在下面。
2. 将能够拦截访问一个（例如www.hitsz.edu.cn）网站的截图和CA被劫持后能够正常访问的截图贴在下面。并分析说明。（建议大家随机选取一个网站，不使用[www.hitsz.edu.cn](http://www.hitsz.edu.cn)）
3. 分析CA证书各密码算法的作用。