ZJGSUCTF 2021 Writeup

B3ale 2021-05-26

Chronos(5)

Category: Misc

- 考察对Linux的熟悉程度以及运维能力
- **docker**：一个开源的应用容器引擎，基于Go语言并遵从Apache2.0协议开源
- `docker pull assassinq/chronos`
- **crontab**：类Unix操作系统命令，用来定期执行程序
- `crontab -e`

Encryptor(10)

Category: Binary

- 考察对逆向调试工具的使用
- GDB：GNU软件系统中的标准调试器
- GDB插件
  - longld/peda
  - pwndbg/pwndbg
  - hugsy/gef

Anti-f5(2)

Category: Binary

- 考察逆向工具的使用以及对常见加密算法的理解
- IDA：Interactive Disassembler公司的反编译与除错工具的产品
- （开源的反编译软件有Ghidra、Cutter等）
- 【技术分享】漫谈几种反编译对抗技术
- **RC4**：一种串流加密法，密钥长度可变，属于对称加密算法

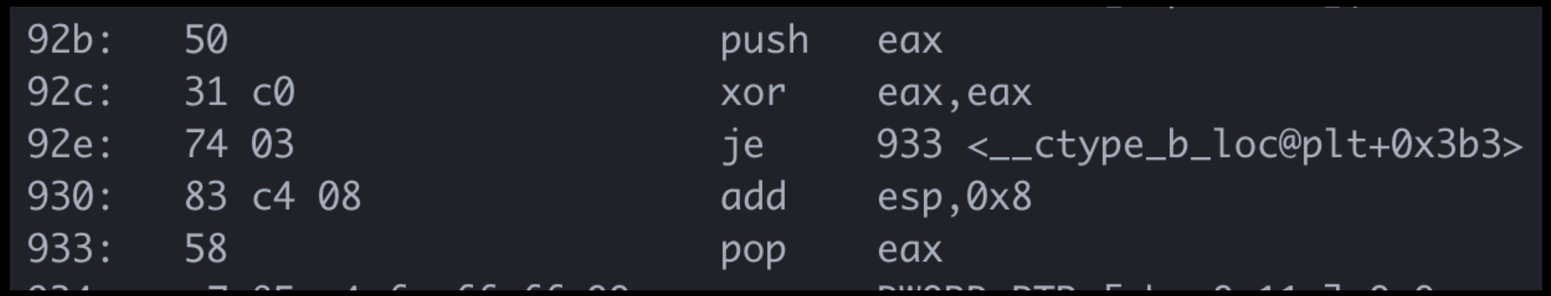
Anti-f5(2)

Category: Binary

```
$ file anti-f5
anti-f5: ELF 32-bit LSB pie executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU
/Linux 2.6.32, BuildID[sha1]=d8dc88e84d5791ed0de12affa93cee65db616b01, stripped
```

Anti-f5(2)

Category: Binary



```
92b:   50                      push   eax
92c:   31 c0                   xor    eax,eax
92e:   74 03                   je     933 <__ctype_b_loc@plt+0x3b3>
930:   83 c4 08                add    esp,0x8
933:   58                      pop    eax
```

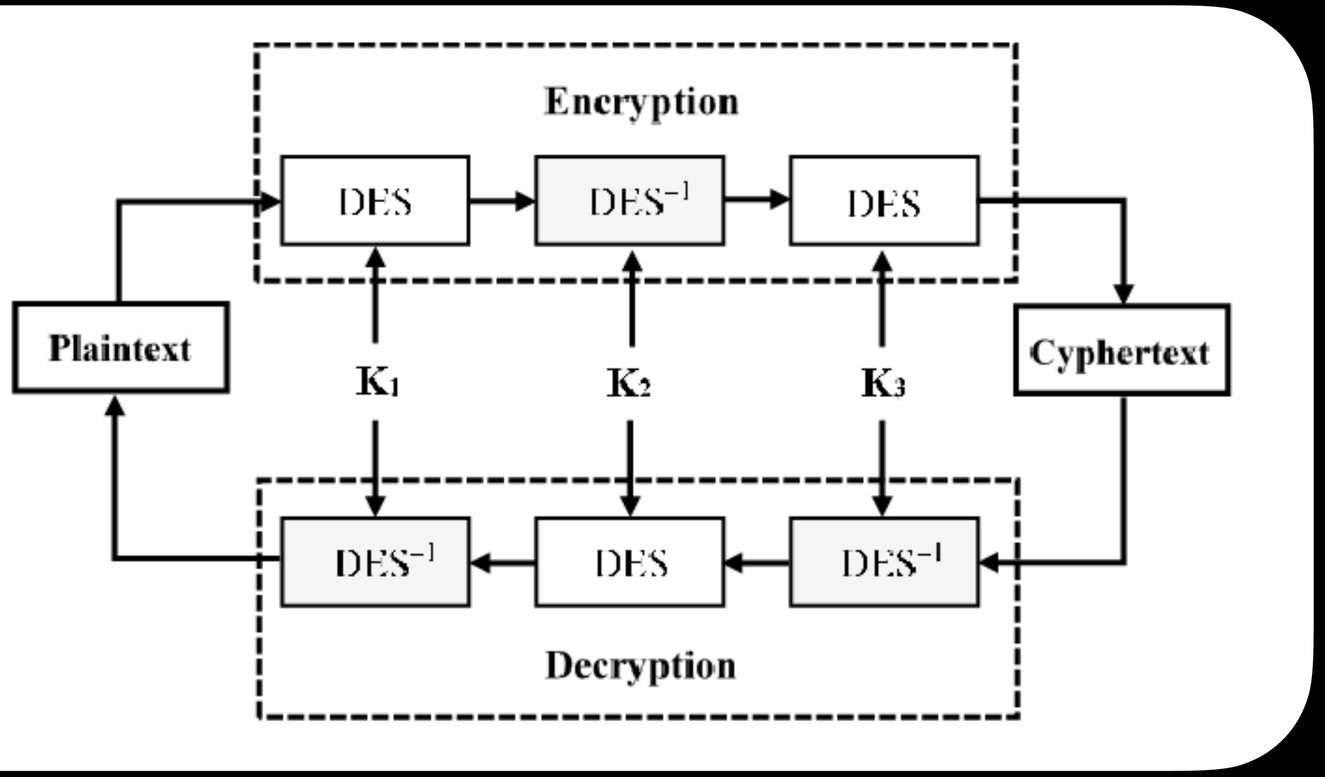
Triple(1)

Category: Crypto

- 考察对DES密码算法的理解
- DES：一种对称密钥加密块密码算法
- 3DES：应用3次DES算法，通过增加DES的密钥长度来避免爆破攻击
- DES子密钥56位，8位**可爆破**
- 参考：NCTF 2019

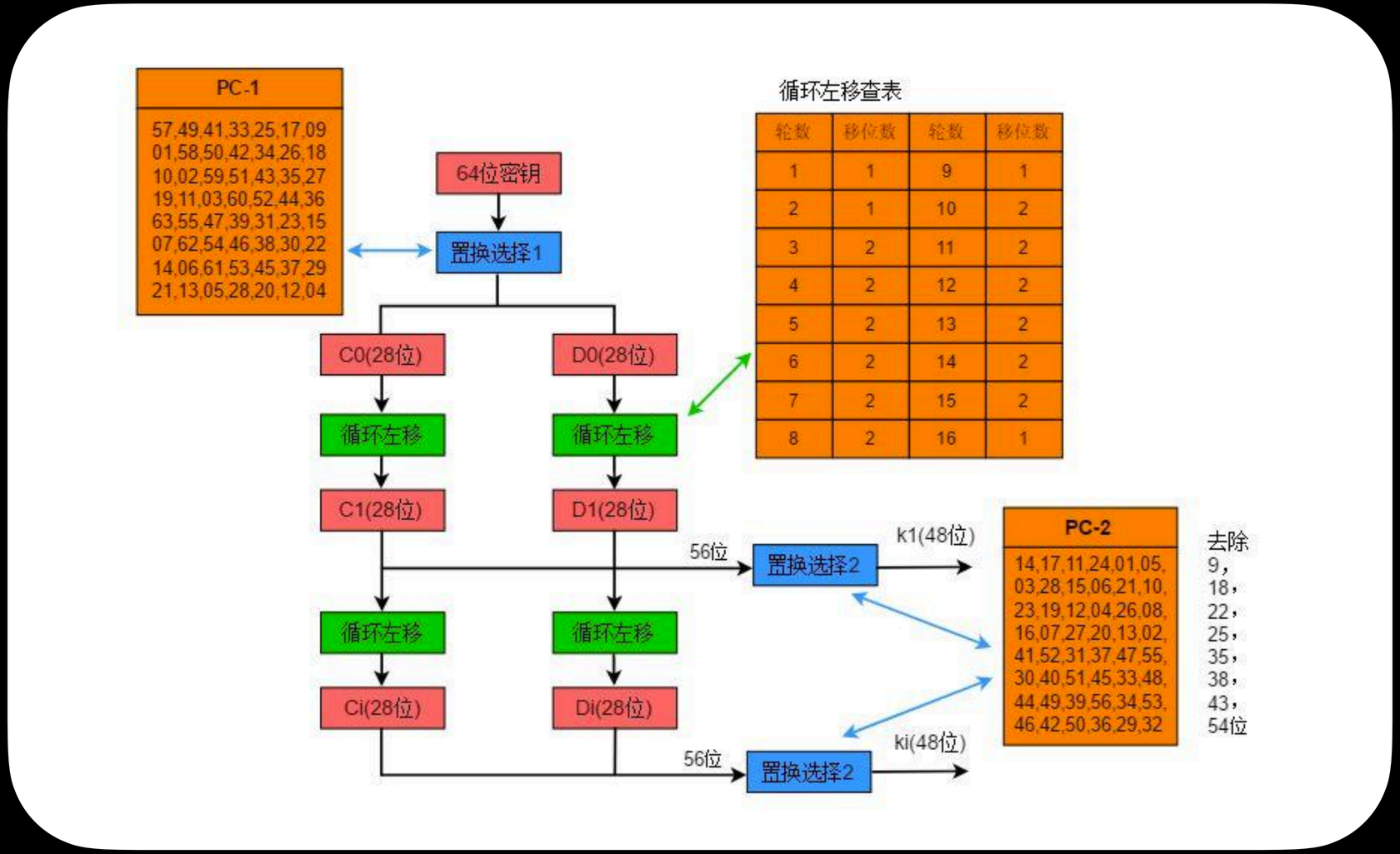
Triple(1)

Category: Crypto



Triple(1)

Category: Crypto



Ezploy(1)

Category: Crypto

- 考察有限域上的多项式运算以及快速学习能力
- 送分题
- 题目中并没有对**多项式**进行加密，密文就是明文
- 参考：2019年第五届上海市大学生网络安全大赛

Lattice(0)

Category: Crypto

- 考察对**格基规约算法**的理解以及快速学习能力
- **RSA**：一种非对称加密算法
- 格基规约算法
- 参考：从一道CTF题初探NTRU格密码

Thank you

B3ale 2021-05-26