CRACK CRYPTO FROM SOURCE

[Publish Date]

European Cyber Security Challenge 2018
London, United Kingdom

1. Initial Write-Up

Even when a crypto system uses AES there can be flaws in it that can be exploited to decrypt data. You have been supplied with the source of a program that generates keys, encrypts data and decrypts data.
The key generation routine has been used to generate a key, and that key has been used to encrypt some text data:

```
$ ./crypto keygen > key
$ cat message | ./crypto enc `cat key` > cipher
```

2. Challenge specifications

- Category: Crypto

3. Tools needed

Description:

Tools needed for the solution of the challenge:

- General Linux tools

4. Walkthrough (writeup)

Keys should be provided as hex strings.

Key:

d366288d4490e99553a909c98f7c2947

Message MD5:

93377af9b652b12ee2351ecad517c96a

(swordfish.txt)