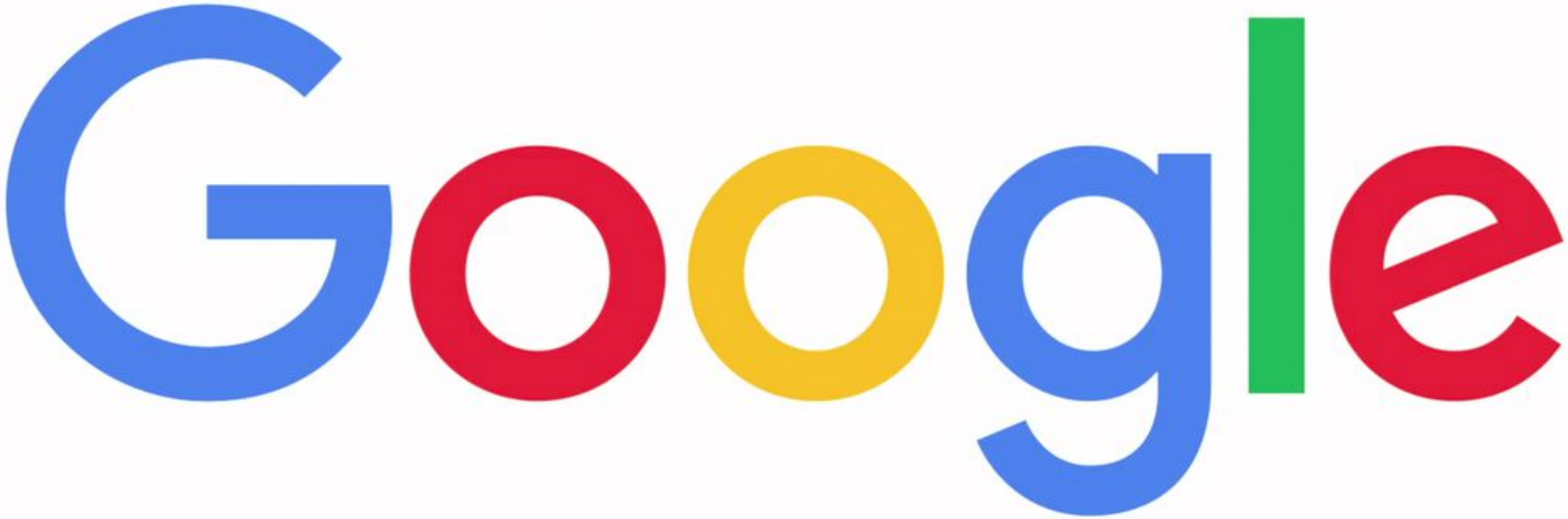
Криптография в CTF

Андрей Гейн

Теория

Исторические шифры
Понятие шифра и ключа
Алгоритм Диффи-Хеллмана
RSA
Электронно-цифровая подпись

Практика


Google

Практика

Plain text и cipher text

Modulus, private и public exponent

Практика: Python

python и ipython

pip install ...

Практика: Python

1 + 2

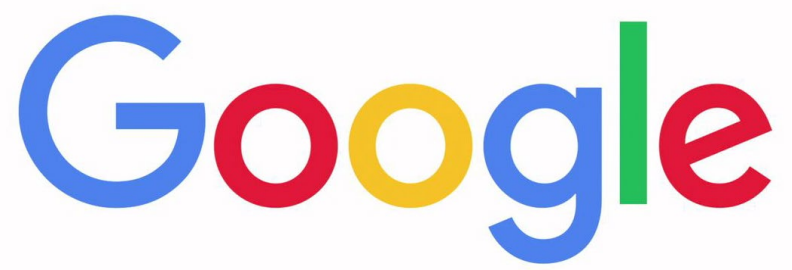
0x1a7f + 123 + 0x7b8a

hex(2733) и '%02x' % 2733

int('1a7f', 16)

2 ** 10 и pow(2, 10, 5)

Нахождение обратного




```
import gmpy2
gmpy2.divm(1, e, n)
```

https://www.lfd.uci.edu/~gohlke/pythonlibs/#gmpy

Число в строку

```
import binascii

number = '48656c6c6f'
binascii.unhexlify(number)

binascii.hexlify(b'Hello world!')
```

Как подключиться

nc и telnet

import socket
socket.create_connection(...)

Берегись врайтапов!

p.andgein.ru