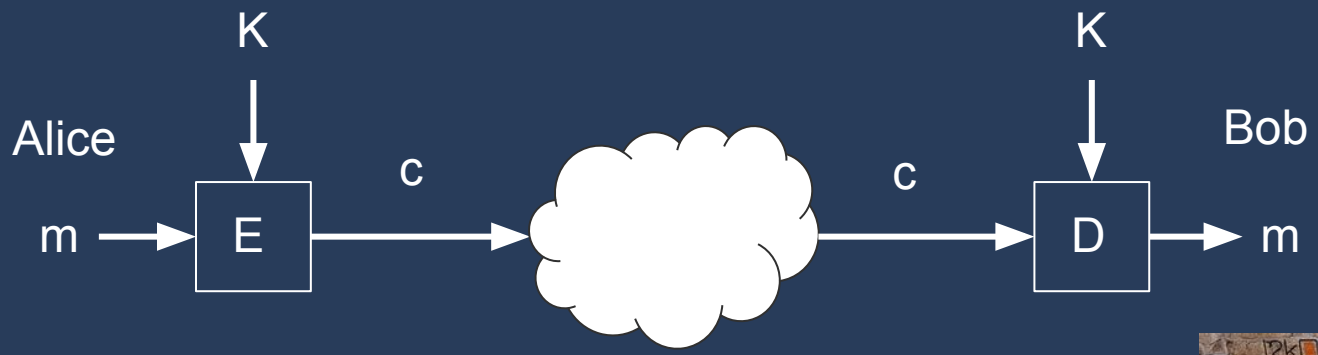
Classic Crypto

2022-04-13

Mattias Grenfeldt

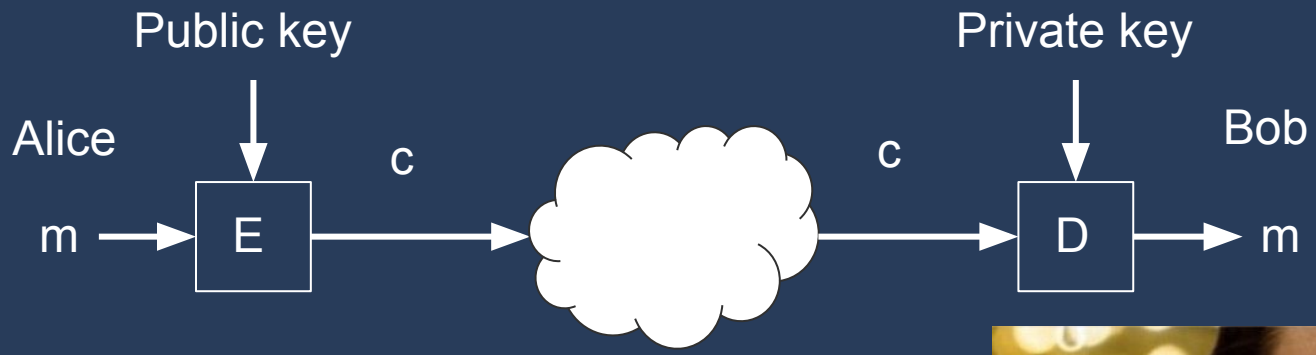
Symmetric Crypto



Exempel:

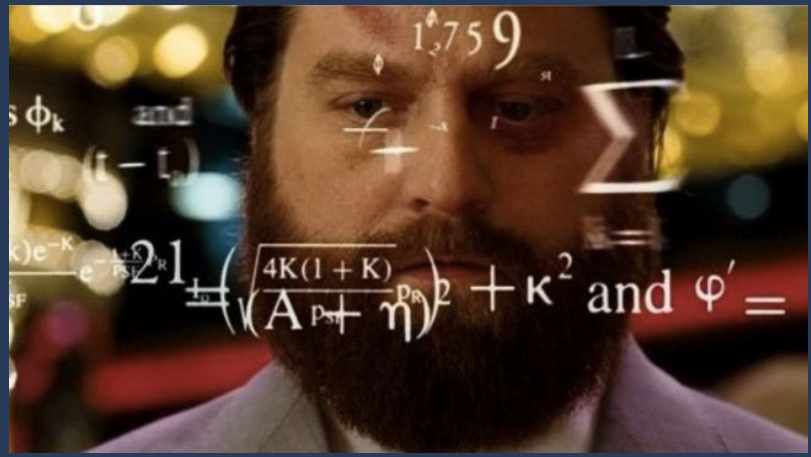
- Classic ciphers
- AES
- DES
- Blowfish
- RC4
- Salsa20

Asymmetric/Public Key Crypto



Exempel:

- RSA
- Diffie-Hellman
- ElGammal
- Elliptic-curve cryptography (ECC)



Caesar Cipher

$$E(m) = m + k \mod 26$$

$$D(c) = c - k \mod 26$$

- Caesar Cipher: k = 3
- ROT13: k = 13
- How to break?
  - Bruteforce k

Substitution Cipher

Vigenere Cipher

XOR

- Exclusive or: ^ ⊕

Truth table	0	1
0	0	1
1	1	0

```
   6 = 110
   3 = 011
 ------------
6^3 = 101
```

- x ^ x = 0
- x ^ 0 = x

One-time pad

- Message (n bits): m
- Random key (n bits): k
- c = E(m) = m ^ k
- m = D(c) = c ^ k
- Totally secure!

		0	1
	Probability	1/2	1/2
0	1 - p	1/2*(1 - p)	1/2*(1 - p)
1	p	1/2*p	1/2*p

Probability of 1:
1/2*p + 1/2*(1 - p) = 1/2

Tools in practice

- https://quipqiup.com/
- https://www.dcode.fr/
- https://www.rictin.com/caesar
- https://daydun.com/ctf/tools/mtp/

Problems

- royalroppers.team/problems/crypto_rsa101.pdf
- royalroppers.team/problems/crypto_the_combine.pdf