Breaking RSA to Pop Shells

with avantika

~# whoami

avantika (@iamavu)

- a girl who dabbles in security
- makes music sometimes
- loves memes :D

what we hacking today?

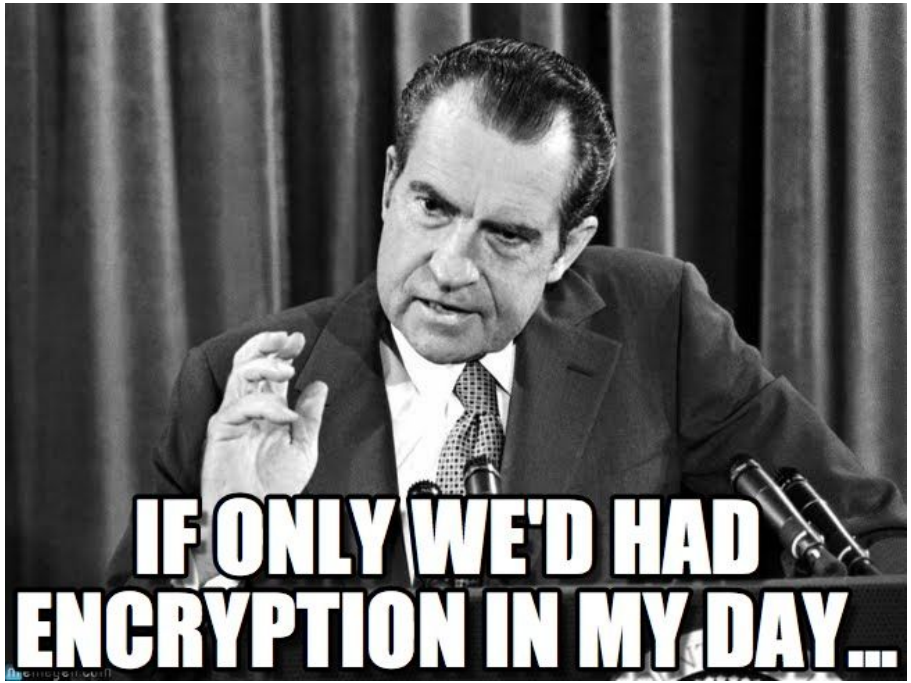
- enumeration
- symmetric encryption
- asymmetric encryption
- rsa
- maths
- python scripting
- fermat attack

enumerate me too

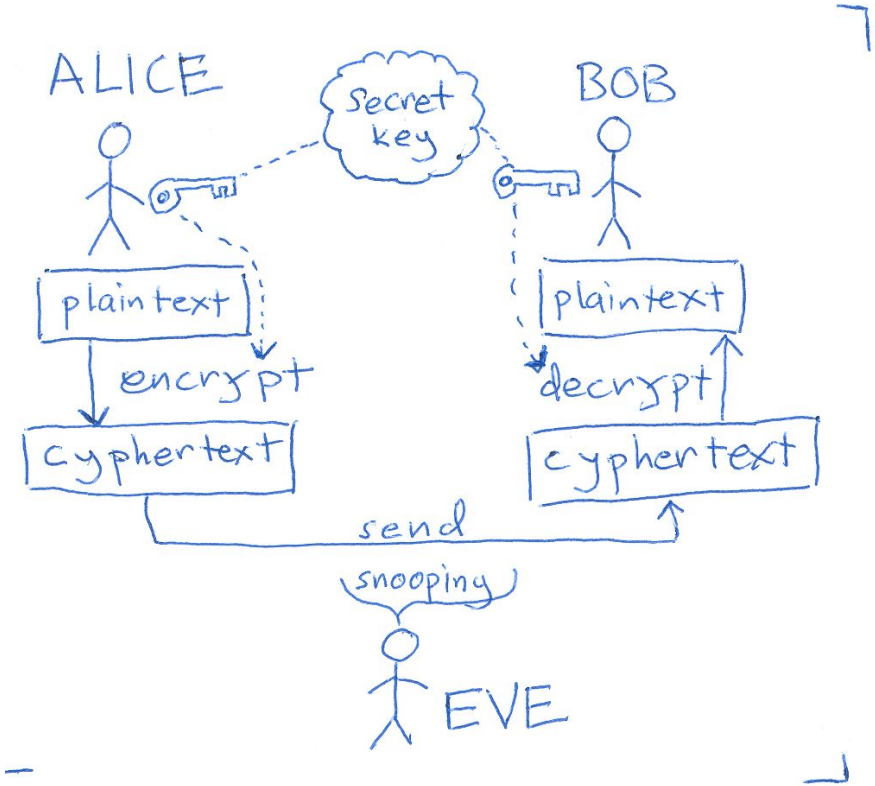
- enumerate
- enumerate
- enumerate
- ....
- ....
- ....
- ....
- enumerate

demo s1

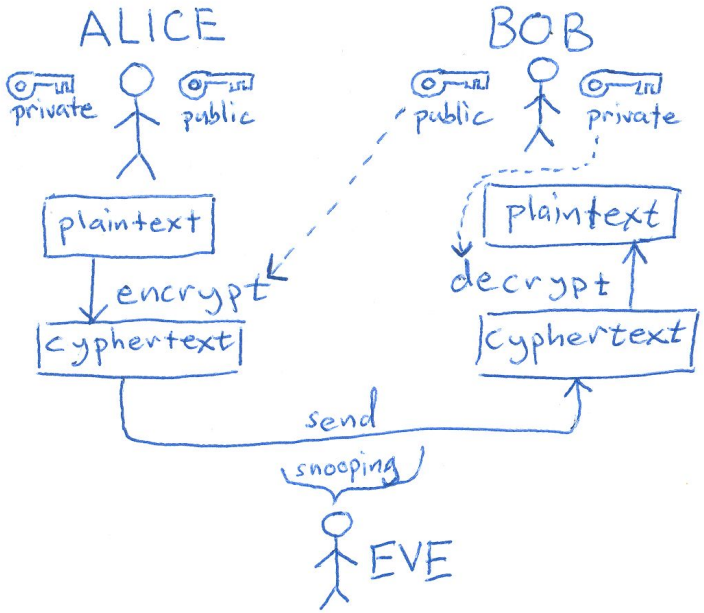
public key? what's that?

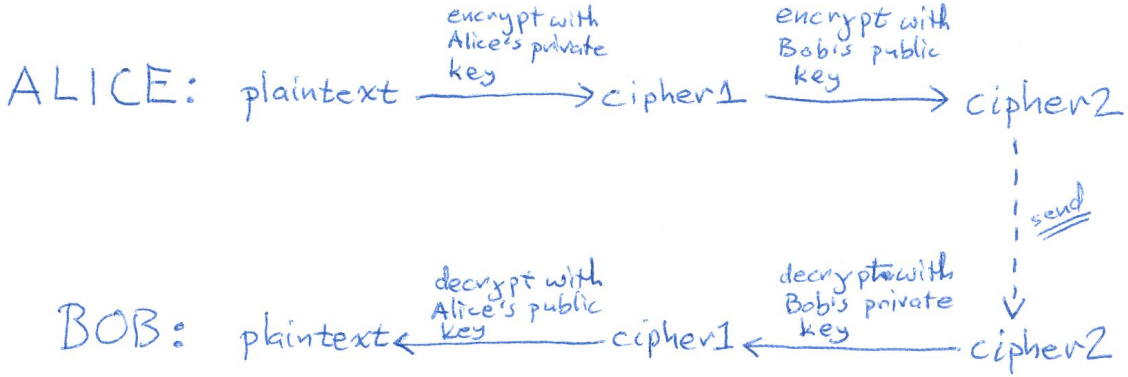


learn with bob,alice and eve season 1 : symmetric encryption



learn with bob,alice and eve season 2 : asymmetric encryption





prime numbers that keep your messages safe

- select two primes (p & q)
- multiply primes to get n (modulus)
- select e, non-factor integer of n (usually 65537)
- public key == (n, e)
- calculate phi = (p - 1) * (q - 1)
- find d such that d * e = 1 % phi
- private key == (d)

demo s2

script me up mom!

- easy as it is almost english
- great community support
- amazing modules/libraries

"You can't just copy-pase pseudocode into a program and expect it to work"

attack it with fermat

- $n = a^2 + b^2$
- $n = (a + b) * (a - b)$
- $a \approx \sqrt{n}$
- $p == a$
- $q == n / a$

demo finale

it is raining shells

r/ask_me_anything