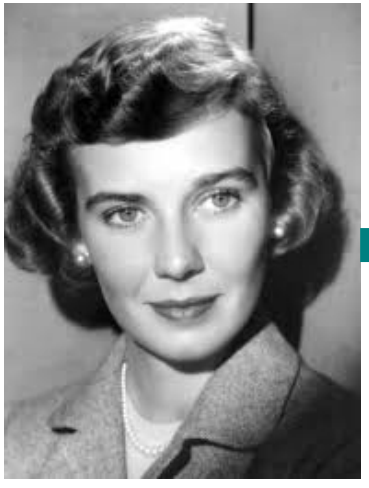
Cryptography : how to talk in a secret language in public

You broke my heart

♥ !

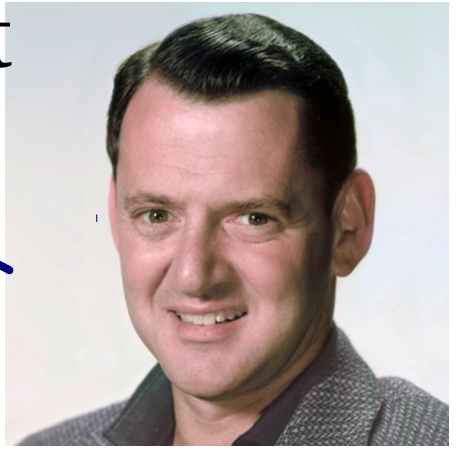
Agreeing on a secret language : Diffie-Hellman



Only Alice knows the combination

Alices' public lock box

Bob's secret language



Bob slams the door

More dials means more possible combinations

Attack times :

D-H 768 bits:
37000y.CPU

D-H 1024 bits:
45 000 000y.CPU

D-H 3072 bits:
ANSSI recommended
(Fill the solar system with CPUs and wait 10bn years)

[Source : Logjam paper (Adrian & al)]

Weight and diversity issues

DH 3072 bits

Same security

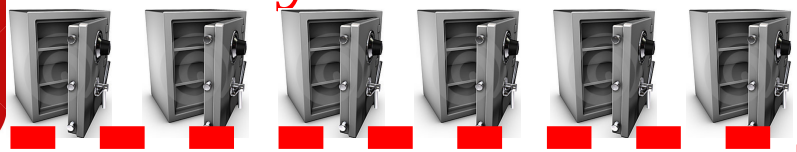
[ANSSI, RGS-Annexe B1]

Ell. curve DH 256 bits

First attack on DH :
45 000 000y.Cpu

Next attacks on similar lock boxes:

0.1y.CPU



Logjam paper : Problem for 26 % Https sites & SSH servers

In real life : downgrade attacks on Diffie-Hellmann

Bob, it’s Alice, let’s use this small lock box

Ok !

Alice — False Alice — Bob

FREAK – SLOTH – LogJam attacks on TLS

See papers of K. Barghavan & al

Listen to science while it is still time!

The death of SHA-1's hash function (1995) :

2005 — Wang & al (CRYPTO)
Theoretical weaknesses

2013 — Stevens (Eurocrypt)
First theoretical attack

2017 — Bursztein & al
First real attack
https://shattered.io/

Firefox awakes

Take-home points

- Check/update your security every ~3 years with the recommendations :

  https://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf
- And beyond standard cryptography:
  - Fragmentation of secrets
  - Blockchain
  - « Trusted computing » (for dedicated tasks)
  - … and be ready when research will provide post-quantum crypto solutions.