Logjam: new dangers for secure protocols

Dmitry Belyavskiy, TCI

ENOG 9, Kazan, June 9-10, 2015

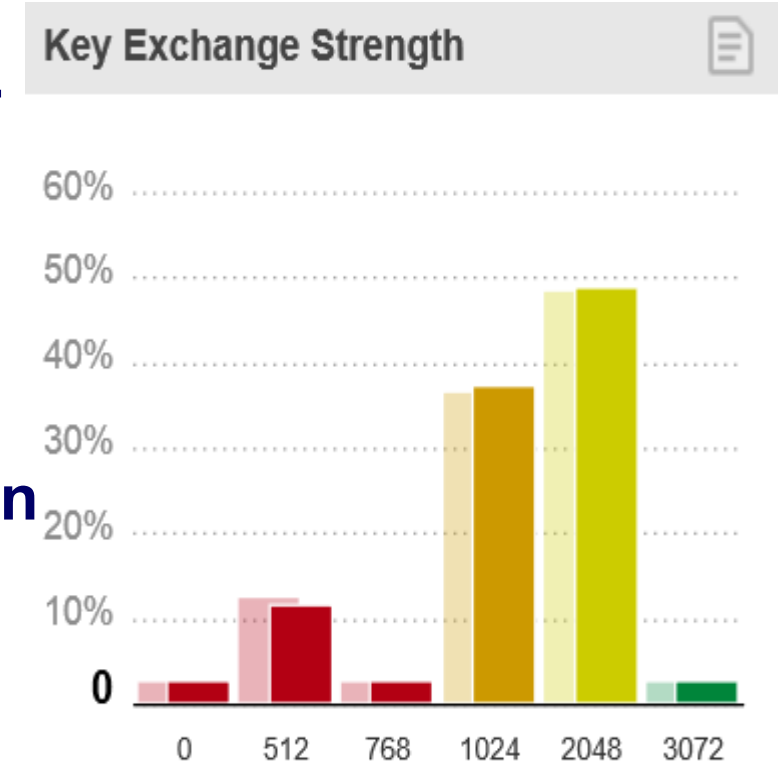
Attack of 2015 – FREAK

- Historical reasons
- A lot of browsers
- A lot of web-servers
- 512-bit temporary RSA is not secure!
- CVE-2015-0204

Fig. 2: FREAK exploit on Safari

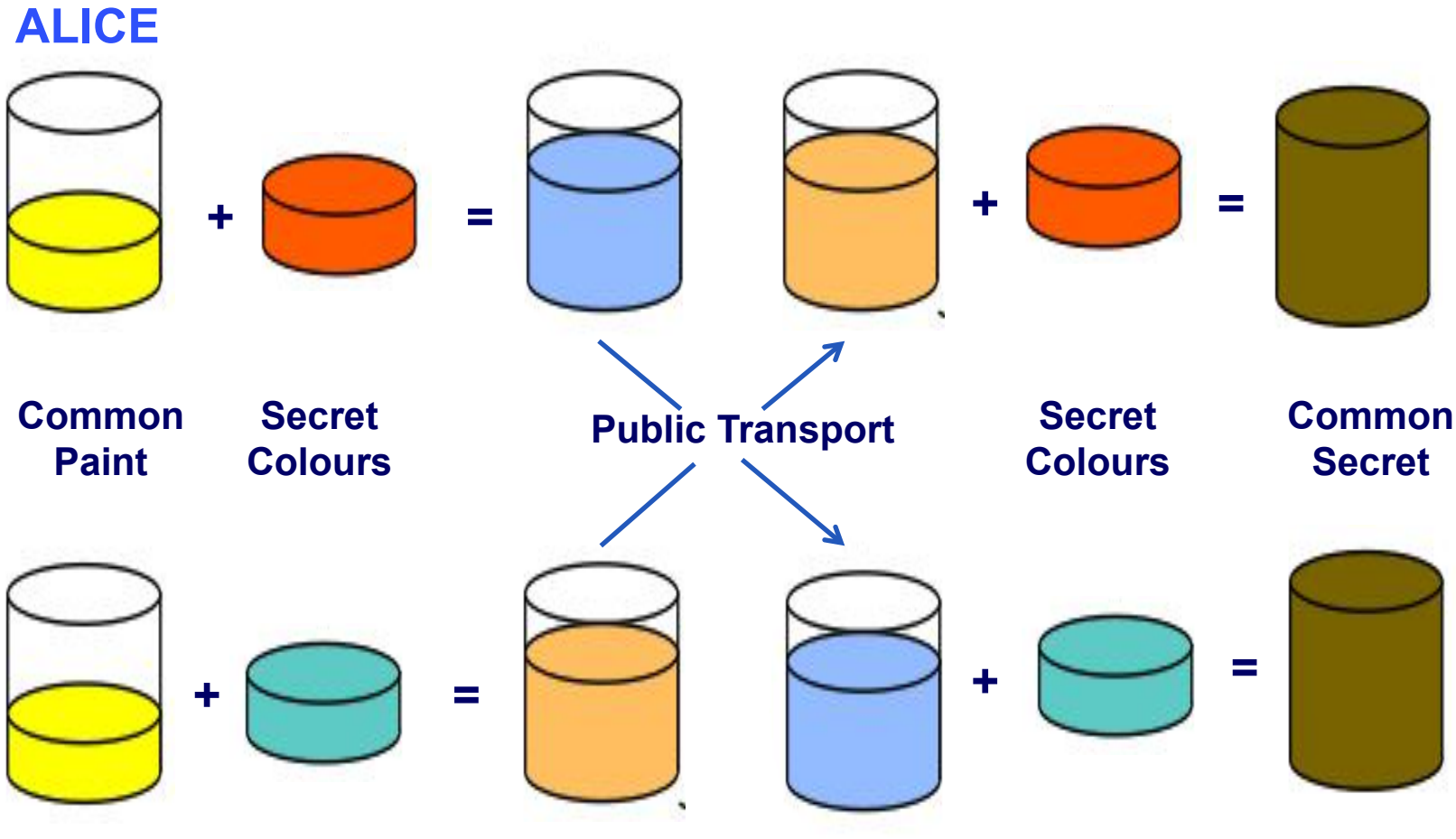
Attack of 2015 – LogJam

- In short: too weak Diffie-Hellman parameters (EXPORT DH)
- All browsers (middle of May)
- All web-servers (depending on settings)
- SSH/VPN
- 512/768/1024 is not enough!



https://weakdh.org/
https://openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes/
https://www.trustworthyinternet.org/ssl-pulse/

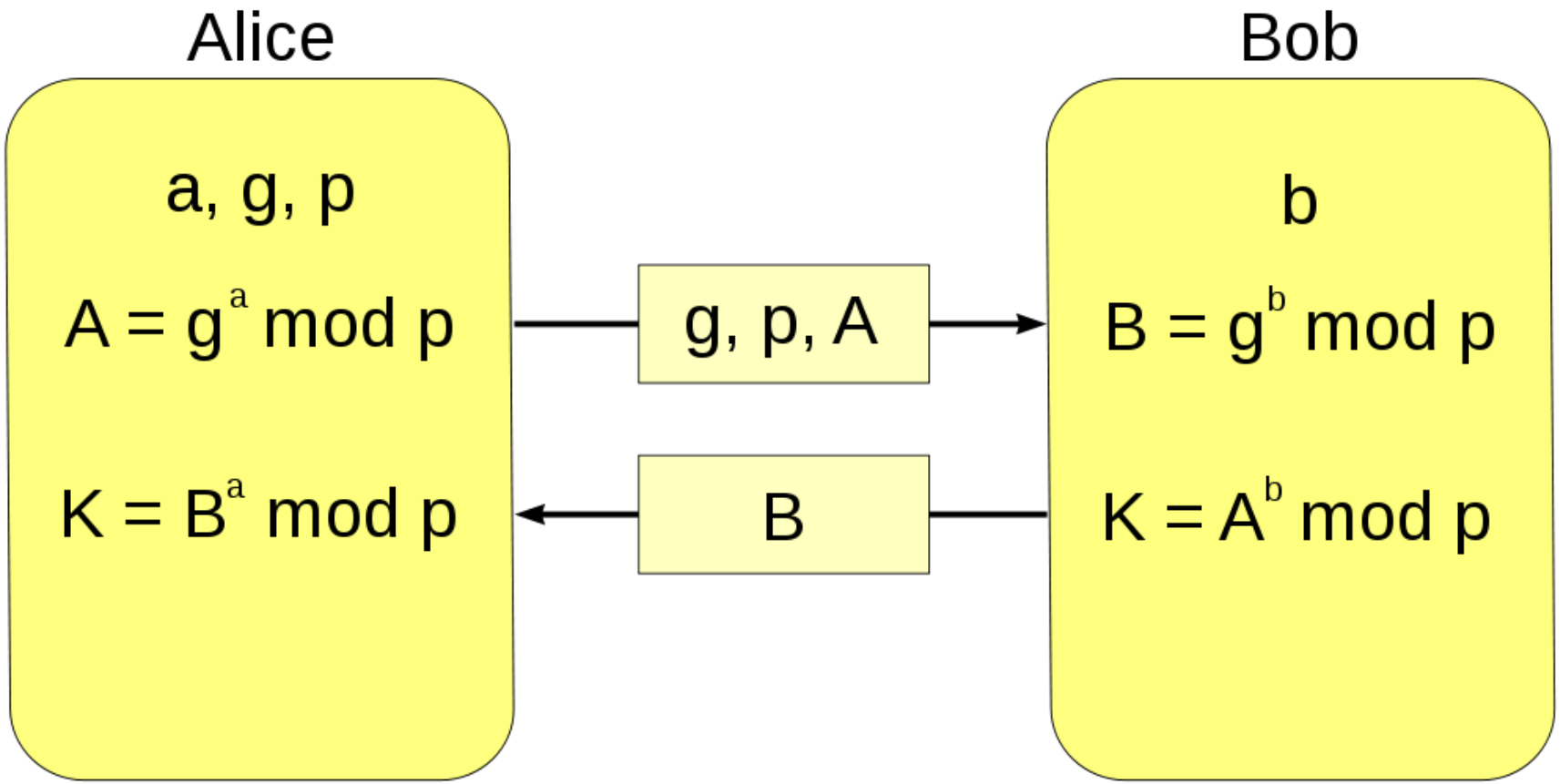
Diffie-Hellman scheme



SSL Best Practices

https://www.ssllabs.com/projects/best-practices/

Diffie-Hellman math

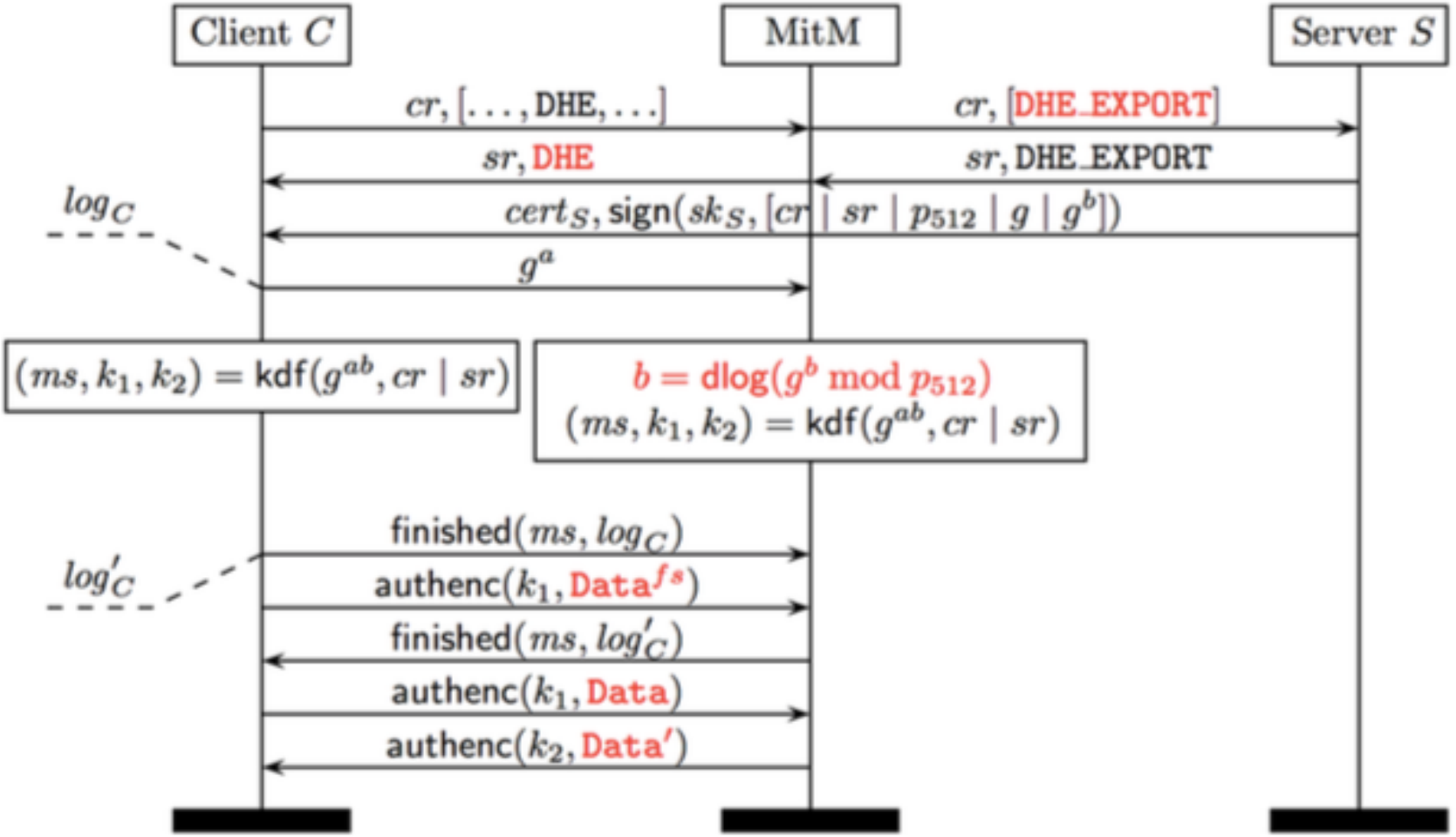


$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Handshake struct

- In case of DH key exchange signed data includes:
  - ✓ opaque client_random[32];
  - ✓ opaque server_random[32];
  - ✓ serverDHParams params;
- DOES NOT include the negotiating Cipher Suite id
- The result will be checked at the end of the handshake

Handshake in case of attack



Why does it work?

- Too short parameters:
  - ✓ Precalc for hard-coded values
  - ✓ Add some timeouts to provide correct Finished message
  - ✓ Profit!
- 2 primes used at 92% Apache sites
- 512 bits is too short
- 1024 bits can be attacked too

Who is under the attack?

- SSH - 25% if 1024 bits is broken
- IKEv1 (IPSEC VPNs) – 66% if 1024 is broken
- HTTPS (7% popular sites)
- IPSec
- POP3S/IMAPS/SMPTP 8-15%

  Postfix enables EXPORT Ciphersuites by default
- … all protocols using DH scheme

How to avoid the attack?

- Switch to ECDH scheme
- Clients should decline too short DH parameters
  - Old Java versions – not longer 768 bits
- Use longer custom parameters (2048 bits)

Questions?

beldmit@tcinet.ru