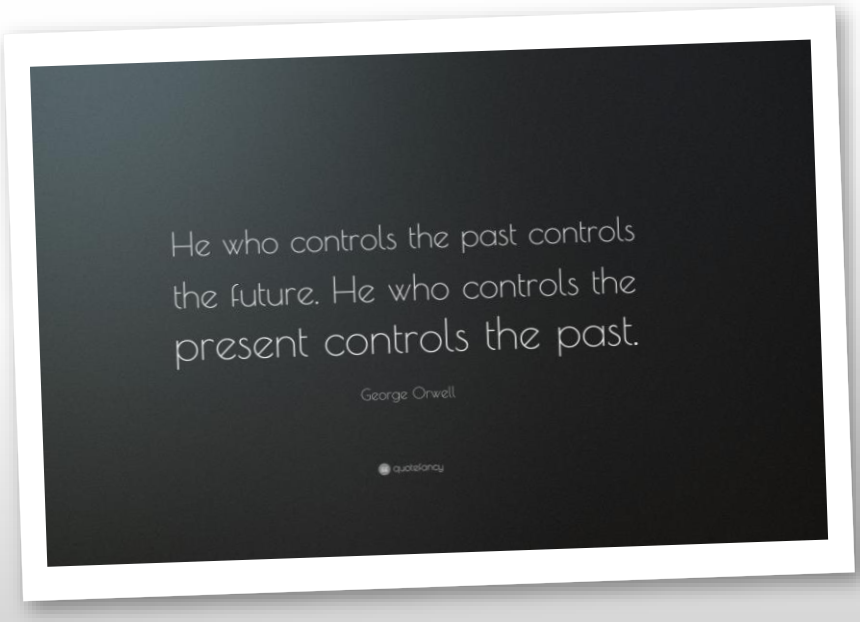
Perfect Forward Secrecy

Gianluca Dini
Department of Ingegneria dell'Informazione
University of Pisa
Email: gianluca.dini@unipi.it
Version: 2022-05-11

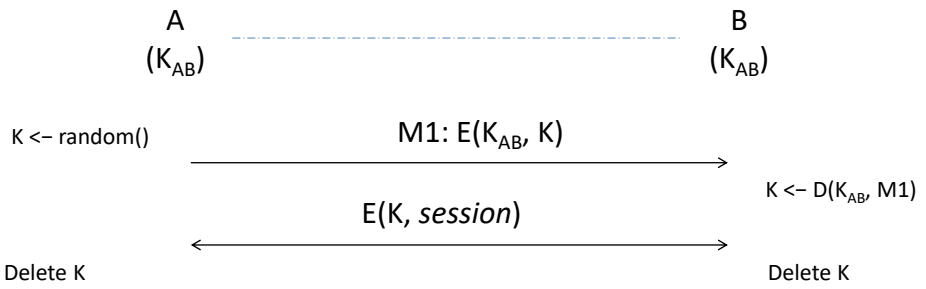
1



2

Pre-Shared Key-based Key Exchange

Warning: replay is not considered for simplicity



- Pre-shared Key K_{AB} is a *long-term pre-shared* secret
- Key K is the *session* key

3

The problem

- The adversary records the encrypted session
- If the adversary compromises the PSK K_{AB} then (s)he can now recover K from M1
- Then, the adversary decrypts the session and violates secrecy
- The long-term secret/key K_{AB} becomes a single-point of failure

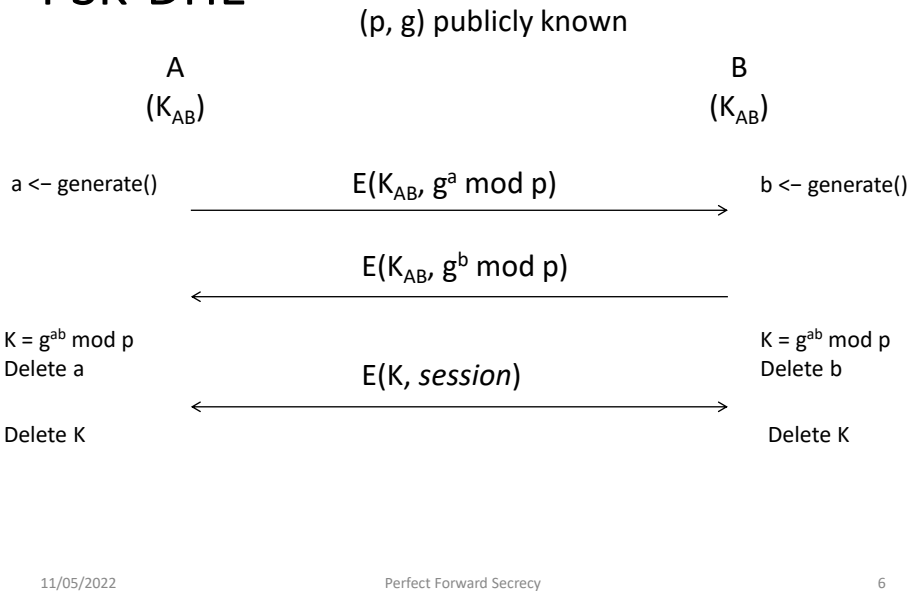
4

Perfect Forward Secrecy

- **(DEF) Perfect Forward Secrecy**
  - Disclosure of long-term secret keying material does not compromise the secrecy of the exchanged keys from earlier runs
- Public Key Cryptography makes it possible to achieve this requirement

5

PSK-DHE

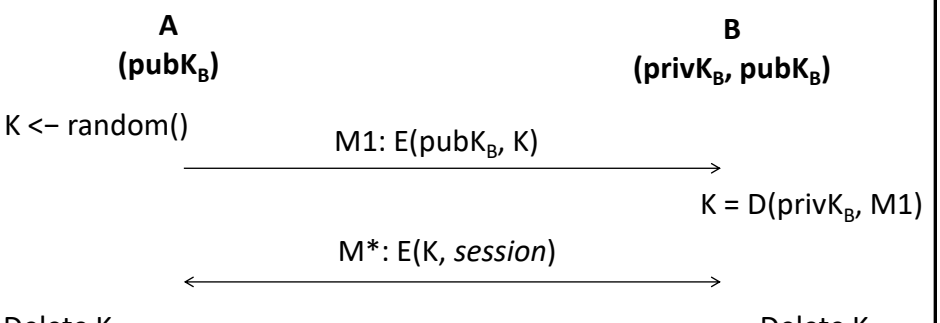


6

PSK-DHE

- Pre-Shared Key Ephemeral Diffie-Hellman
- Ephemeral Diffie-Hellman
  - Keys a and b are ephemeral
    - One-time (per-session or per message)
  - Once a and b (and K) have been deleted there is no way to recover K, and thus the session, even if the long-term private K_{ab} is compromised: neither A nor B can
- Even though the shared key K_{ab} is compromised, the adversary has still to solve the DLP
  - K_{ab} is used for authentication and not for confidentiality anymore

PKE-based Key Exchange



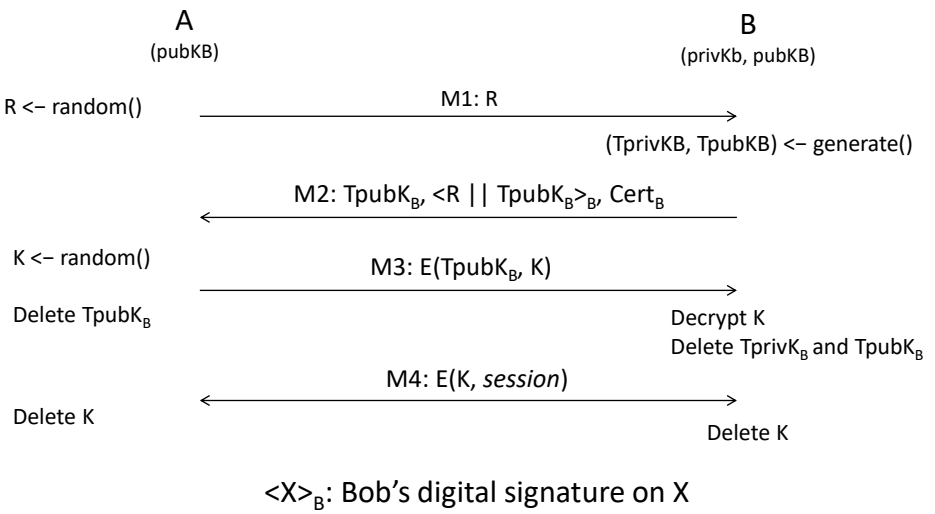
- Private key $privK_B$ is a *long-term* secret
- Key K is the *session* key
- SSL/TLS employs a similar scheme

The problem

- The adversary records the encrypted session
- If the adversary compromises $privK_B$ then (s)he can recover K from CT
- Then, the adversary decrypts the session and violates secrecy
- The long-term secret becomes a single-point of failure

9

Ephemeral RSA (RSAE)



$<X>_B$: Bob's digital signature on X

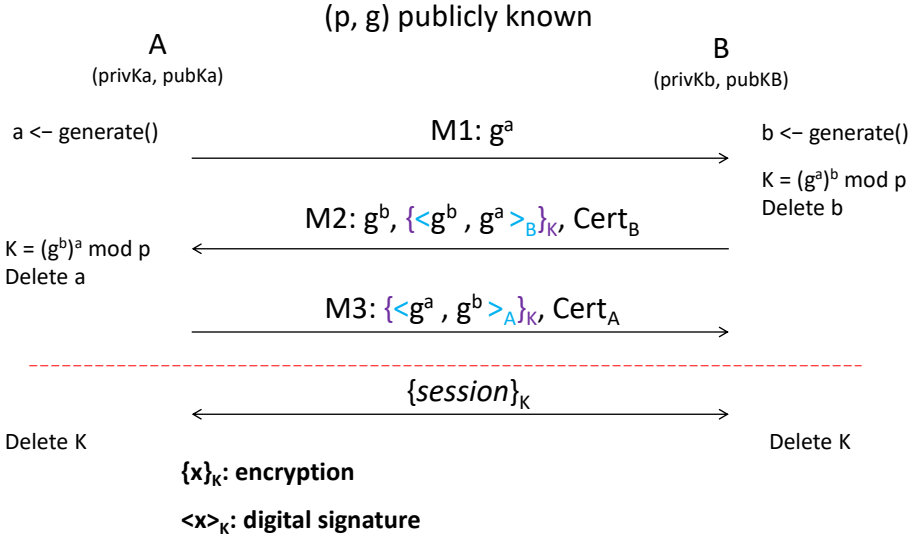
10

Direct Authentication

- (DEF) Direct Authentication: To prove the peer the knowledge of the key K
  - If a Key Exch protocol does not fulfil direct authentication, this authentication is achieved at the first application message
  - DA is also said Key Confirmation in the BAN parlance
- DHE and RSAE don't fulfil direct authentication
  - Until E(K, *session*)
- Station-To-Station (STS) Protocol fulfils direct authentication while guaranteeing PFS

11

Station-to-Station protocol



12

Misc

- CONS
  - PFS requires more computation
  - Crypto-(co)processors do not support PFS (for the moment)
- Who uses PFS
  - Whatsapp, Twitter, IOS9, Google
  - (EC)DHE is part of SSL/TLS cipher suite
- SSL Quality Test
  - https://www.ssllabs.com/ssltest