

# Perfect Forward Secrecy

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

1

He who controls the past controls  
the future. He who controls the  
present controls the past.

George Orwell

quotefancy

11/05/2022

Perfect Forward Secrecy

2

2

## Pre-Shared Key-based Key Exchange

**Warning:** replay is not considered for simplicity

The diagram illustrates a key exchange protocol between two parties, A and B, who share a pre-shared key  $K_{AB}$ . Party A generates a random session key  $K$  and sends its encryption  $M1: E(K_{AB}, K)$  to Party B. Party B then decrypts  $M1$  using  $K_{AB}$  to recover  $K$ . Both parties then use  $K$  to encrypt their session data,  $E(K, session)$ , and send it to each other. Finally, both parties delete the session key  $K$ .

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

11/05/2022 Perfect Forward Secrecy 3

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

11/05/2022 Perfect Forward Secrecy 4

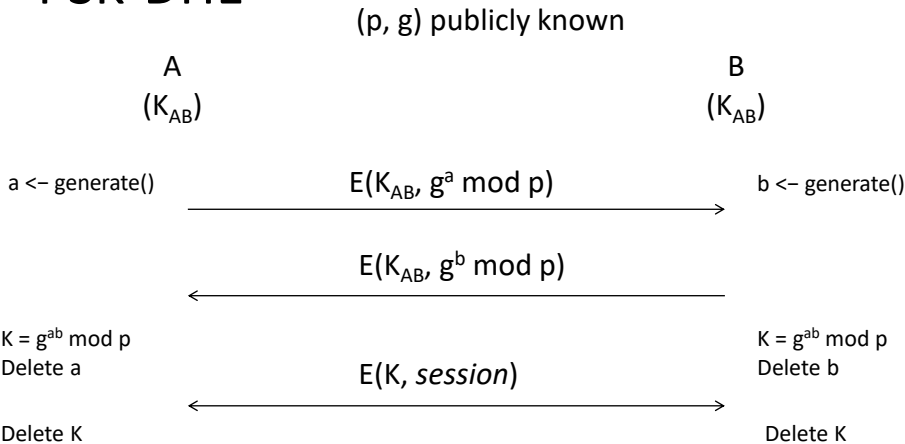
4

# 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



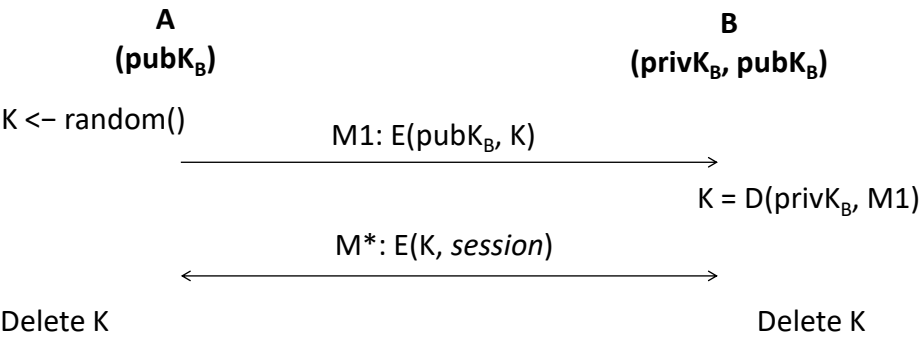
6

# 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<sub>ab</sub>* is compromised: neither A nor B can
- Even though the shared key *K<sub>ab</sub>* is compromised, the adversary has still to solve the DLP
  - *K<sub>ab</sub>* is used for authentication and not for confidentiality anymore

7

# PKE-based Key Exchange



- Private key *privK<sub>B</sub>* is a *long-term* secret
- Key *K* is the *session* key
- SSL/TLS employs a similar scheme

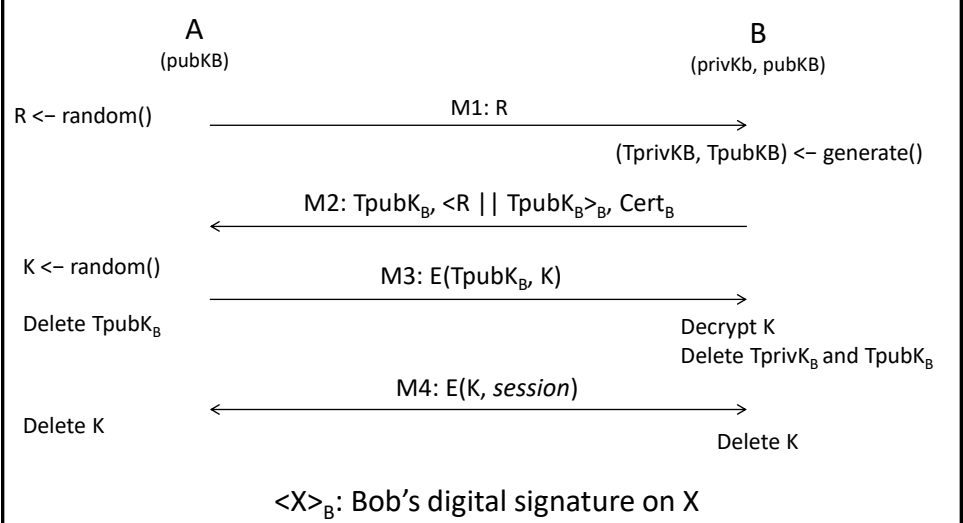
8

# The problem

- The adversary records the encrypted session
- If the adversary compromises  $\text{privK}_B$  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)



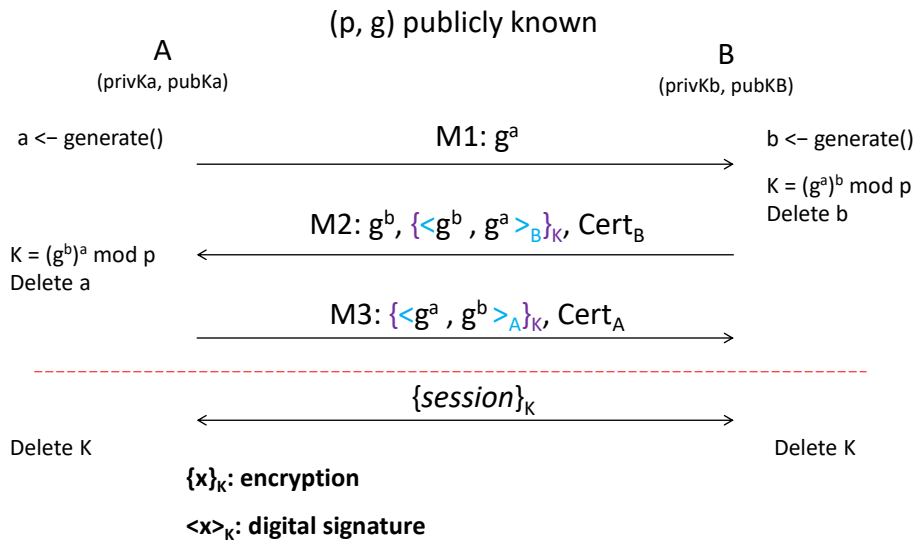
10

# 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>

11/05/2022

Perfect Forward Secrecy

13

13