Perfect Forward Secrecy

Security in Networked Computing Systems

PKE-based Key Ex

A **($pubK_B$)**		**B** **($privK_B$, $pubK_B$)**
K <– random()		
	CT = E($pubK_B$, K) →	
		K = D($privK_B$, CT)
	E(K, *session*) ↔	
Delete K		Delete K

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

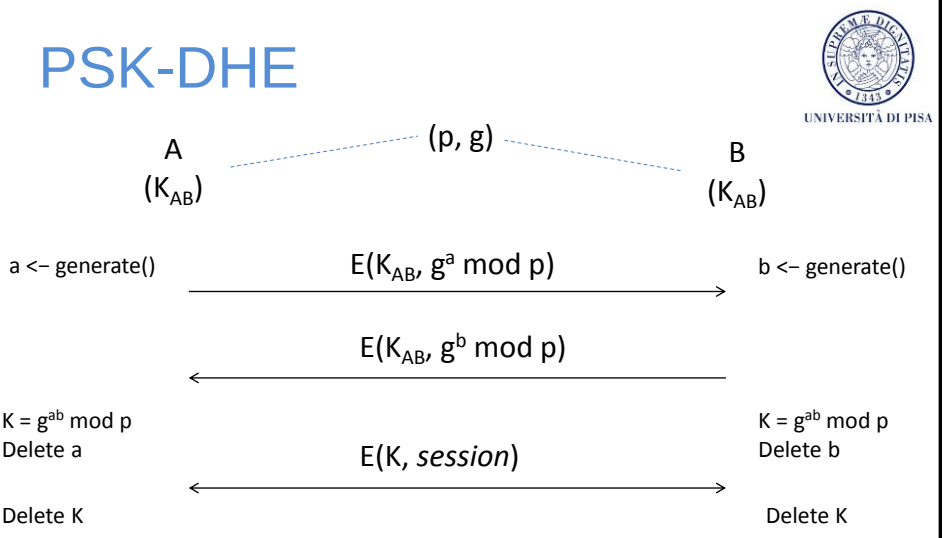
The problem

- The adversary records CTs of the 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

Perfect Forward Secrecy

- **(DEF) PFS**: Disclosure of long-term secret keying material does not compromise the secrecy of the exchanged keys from earlier runs
- PKE, and in particular DH, makes it possible to achieve this requirement

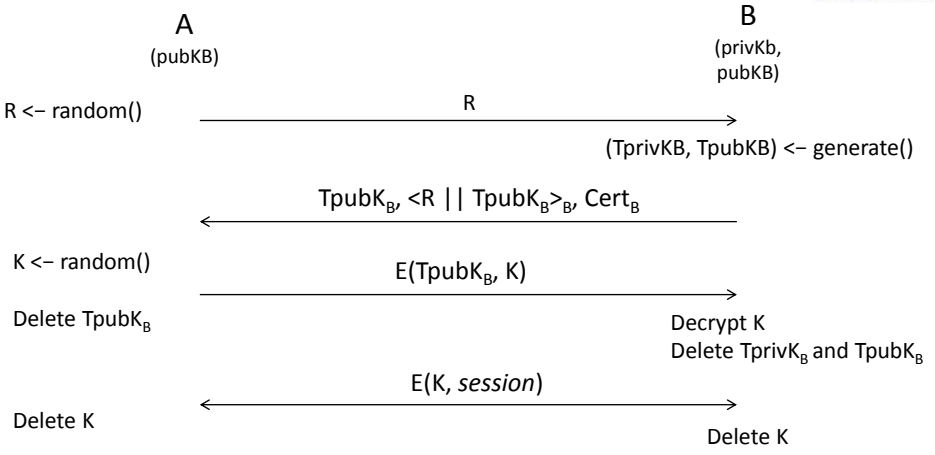
PSK-DHE



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 private K_{ab} is compromised, you still have to solve the DLP

Ephemeral RSA (RSAE)

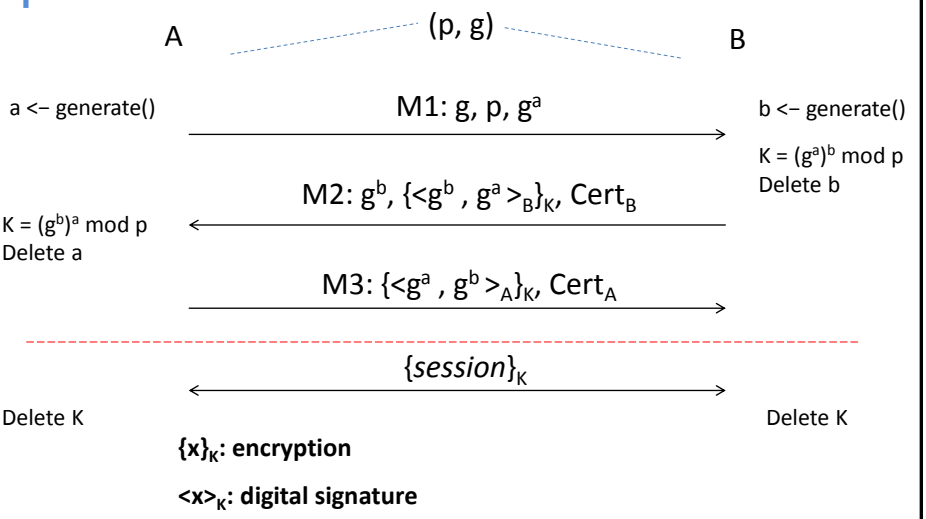


$<X>_B$: Bob's digital signature on X

Direct Authentication

- (DEF) **Direct Authentication** means to prove the peer the knowledge of K
  - If a KeyEx protocol does not fulfil direct authentication, this authentication is achieved at the first application message
  - DA is 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

Station-to-Station (STS) protocol



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