DIFFIE-HELLMAN KEY EXCHANGE
Lecture 7d

COMPSCI 726
Network Defence and Countermeasures

Muhammad **Rizwan** Asghar

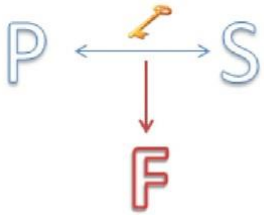
August 2, 2021

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

FORWARD SECRECY

- What if a private key gets compromised?
  - It can reveal
    - Data exchanged in that session and
    - Data exchanged in previous sessions
- Forward secrecy ensures data protection in all previous sessions even if a private key gets compromised
- For achieving forward secrecy, an ephemeral session key is typically derived from a set of long-term public and private keys
- The session key is destroyed after the session!
- Recovering a session key becomes more difficult even if one gets access to the private key

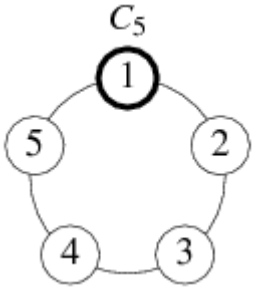
PERFECT FORWARD SECRECY



- Perfect Forward Secrecy (PFS) is a stronger notion of forward secrecy

- PFS ensures that a public key cryptosystem meets two additional constraints
  - For each session, a random key is generated
  - The cryptosystem does not use any deterministic algorithm in generating new keys

FINITE CYCLIC GROUP



- g is a generator of group Z_n^* if
  $Z_n^* = \{g^1, g^2, \ldots, g^{n-1}\} = \{1, 2, \ldots, n-1\}$

- 2 is a generator of Z_5^*
  - $2^1 \equiv 2 \pmod 5$
  - $2^2 \equiv 4 \pmod 5$
  - $2^3 \equiv 8 \equiv 3 \pmod 5$
  - $2^4 \equiv 16 \equiv 1 \pmod 5$

- $Z_5^* = \{2^1, 2^2, 2^3, 2^4\} = \{2, 4, 3, 1\} = \{1, 2, 3, 4\}$

FINITE CYCLIC GROUP: EXAMPLE

- g = 5 and n = 7
- 5 is a generator of Z_7^*
  - $5^1 \equiv 5 \pmod 7$
  - $5^2 \equiv 25 \equiv 4 \pmod 7$
  - $5^3 \equiv 5^1 \,.\, 5^2 \equiv 5 \,.\, 4 \equiv 20 \equiv 6 \pmod 7$
  - $5^4 \equiv 5^2 \,.\, 5^2 \equiv 4 \,.\, 4 \equiv 16 \equiv 2 \pmod 7$
  - $5^5 \equiv 5^2 \,.\, 5^3 \equiv 4 \,.\, 6 \equiv 24 \equiv 3 \pmod 7$
  - $5^6 \equiv 5^3 \,.\, 5^3 \equiv 6 \,.\, 6 \equiv 36 \equiv 1 \pmod 7$
- $Z_7^* = \{5^1, 5^2, 5^3, 5^4, 5^5, 5^6\} = \{5, 4, 6, 2, 3, 1\}$
- Is 3 a generator of Z_5^* ?
- Is 3 a generator of Z_7^* ?

TO BE CONTINUED

- See the next lecture

Questions?

Thanks for your attention!