Secure messaging using SMS

SIRS

MEIC-A
Group 6
70171 - João Miguel Neves
72904 - Luís Ribeiro Gomes
74190 - Ana Beatriz Alves

Problem

- SMS security relies on underlying network security
  - Network provider can look into messages
  - Attacks are possible

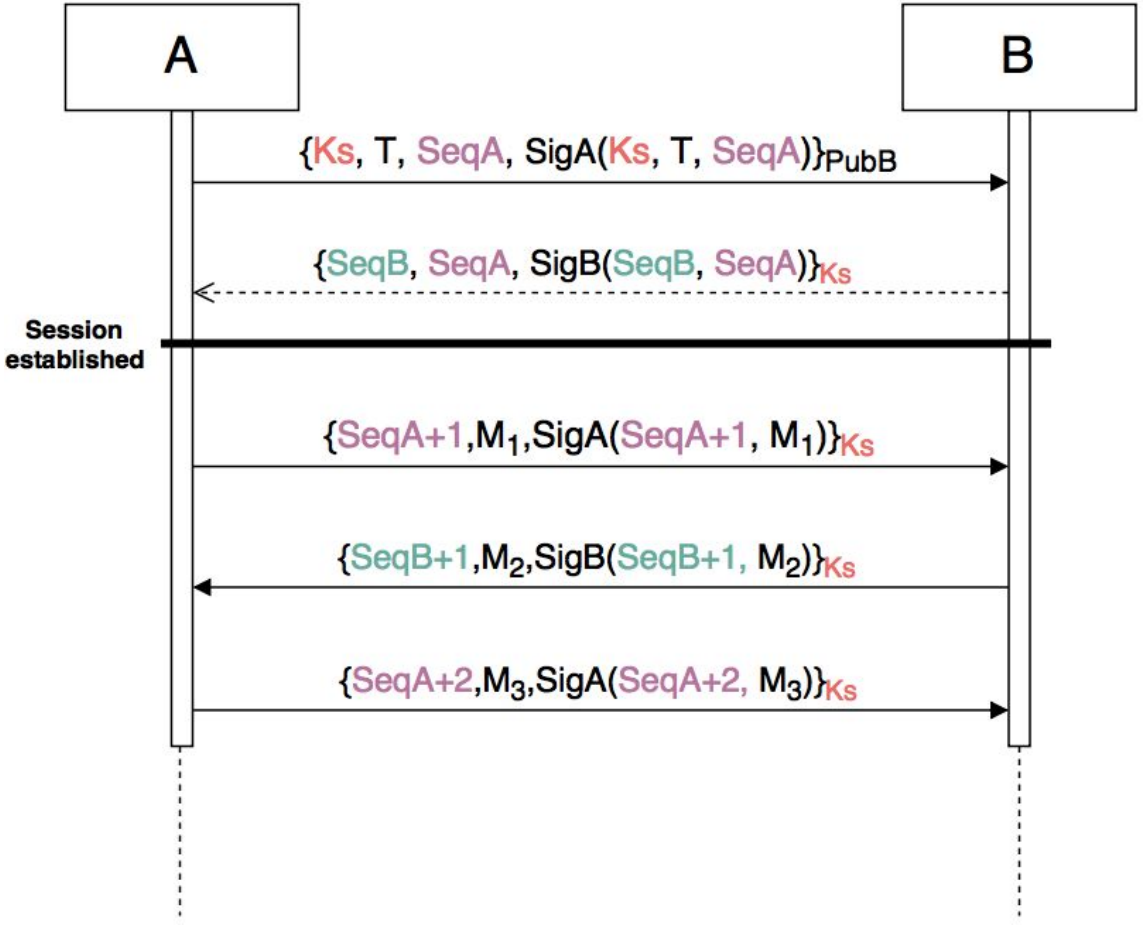
Solution

- Secure messaging must guarantee
  - Confidentiality
  - Integrity
  - Authentication
  - Freshness

Solution - Protocol

- Long term asymmetric keys
- Symmetric session keys

- Signatures
  - Integrity
  - Authentication
- Freshness
  - Timestamps
  - Sequence numbers



Solution - Implementation

- Asymmetric cryptography
  - X.509 Certificates
    - Can be validated by a CA
  - Encryption
    - RSA (2048 bits)
  - Signatures
    - EC (224 bits)
      - Short signatures
      - Fast
- Symmetric cryptography
  - AES in CBC mode with CTS (128 bit keys)
    - New random IV for every message

Solution - Implementation

- Key Storage
  - Bouncy Castle API - Key Store
  - Content - all encrypted
    - Certificates
    - Private keys
    - Session keys

Solution - Implementation

- Application Storage
  - Android API - Shared Preferences
  - Content
    - User info
    - Contacts info
    - SMS info - encrypted
    - Session info

Solution - Architecture