Network and Computer Security

Secure messaging using SMS

Project Plan

MEIC-A
Group 6

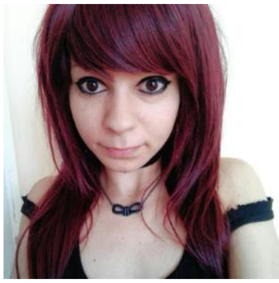
70171

João Miguel Neves

72904

Luís Ribeiro Gomes

74190



Ana Beatriz Alves

Motivation

SMS exchanging has always been insecure due to the lack of security measures.
A message is usually sent in plain-text, which means that anybody can intercept and read it, as well as impersonate someone else.
Security is necessary so that everyone can communicate safely and privately at a distance, using their phones.

Goals

By the end of the development of this project, we expect to obtain an application that allows non-expensive SMS exchanging while taking into account security properties, such as confidentiality, integrity, authentication, non-repudiation and freshness.
In order to do so, we plan to:

- Establish a secure channel in which parties can communicate privately
- Ensure that the message wasn't tampered with
- Prevent replay attacks
- Minimize number of exchanged messages
- Deal with large messages and join partial SMS

Proposed solution

Assumption: There is a reliable data bank where **A** and **B** can obtain each other's public keys.

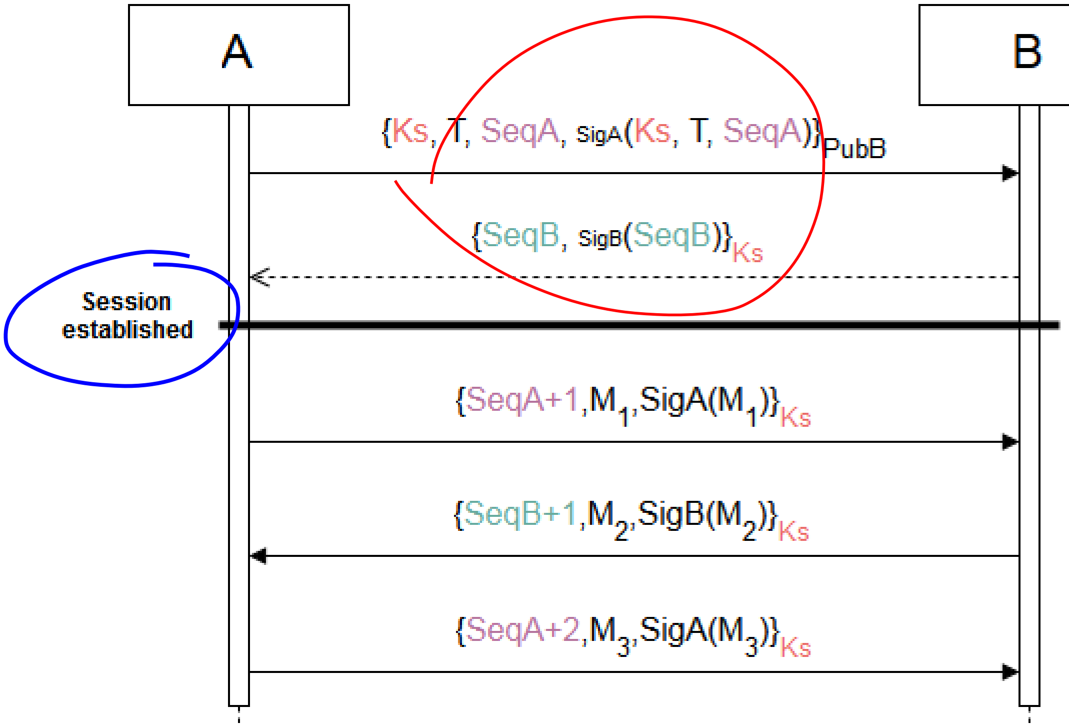
When **A** wants to communicate with **B** (see diagram below):
The session key (Ks) will be used to encrypt every interaction between both parties until the session expires, while the sequence number (SeqA/SeqB) allows **B**/**A** to receive the messages from **A**/**B** (respectively), in the correct order, while ensuring freshness.

To begin the session, the sender attaches a timestamp (T) so it's possible to check its validity - confirming a new session implies that receiver verified whether the session expired, or if there is an active session with the sender using the same timestamp.

After validating the exchanged information, both parties can communicate for the duration of the session, since we achieved:

- Integrity - Hash of the message in the signature;
- Confidentiality - Only readable for those with the session key;
- Authentication - KEK (**A** by signing and **B** by decrypting with their own private keys);
- Freshness - Timestamp and sequence numbers;
- Non-repudiation - Phone number

Diagram



3-2

Work Plan

	70171	72904	74190
02-Nov	- Security protocol scheme	-Security protocol scheme	- Security protocol scheme
09-Nov	- Algorithm definition - Key management	- Algorithm definition - Simple SMS exchanging	- Algorithm definition - Android interface
16-Nov	- Session management	- SMS generation/validation	- SMS generation/validation
23-Nov	- Session management - Long SMS splitting	- SMS generation/validation - Long SMS splitting	- SMS generation/validation - Long SMS splitting
30-Nov	- Long SMS splitting	- Long SMS splitting	- Long SMS splitting

Tool References

Java SE

Android SDK Tools

Bouncy Castle Crypto API

Notes

2-1 Requires attacking the network

2-7 Explain better

3-2 Relation of seqa with seqb

Session pairing?