Cristina Nita-Rotaru

CS355: Cryptography

Introduction

Course information

- Meetings
  - MWF 12:30-1:20 LWSN 1106
  - Make up class: Monday at 6 pm in same room, TU 6 pm in LWSN B 146. We will use the lab for exercises in class.
- Professor contact info:
  - Office: 2142J
  - Email: crisn@cs
  - **Office hours: by appointment**
- TA: Denis Ulybyshev
  - Email: dulybysh@purdue.edu
- Class webpage
- http://homes.cerias.purdue.edu/~crisn/courses/cs355_Fall_2012/
- Use Piazza for questions and postings

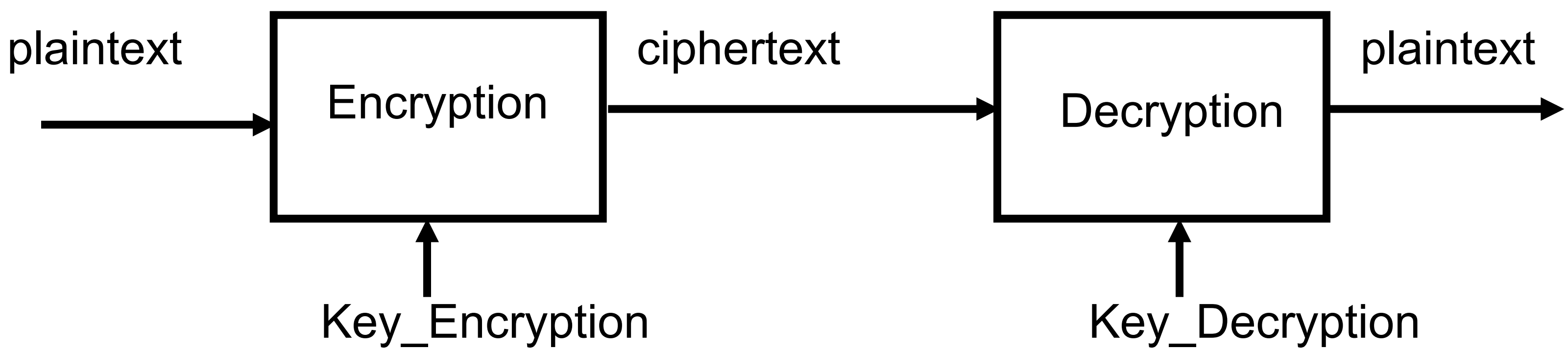
The science of secrets…

- **Cryptography:** the study of mathematical techniques related to aspects of providing information security services (create)
- **Cryptanalysis:** the study of mathematical techniques for attempting to defeat information security services (break)
- **Cryptology:** the study of cryptography and cryptanalysis (both)

Basic terminology in cryptography

- cryptography
- cryptanalysis
- cryptology

- plaintexts
- ciphertexts
- keys
- encryption
- decryption



Cristina Nita-Rotaru

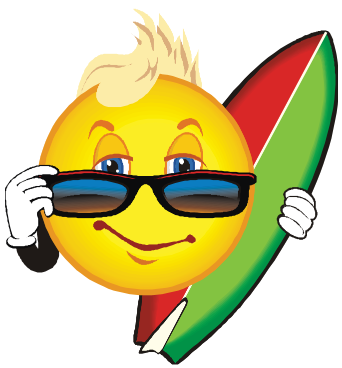
Cryptographic protocols

- Protocols that
  - Enable parties
  - Achieve objectives (goals)
  - Overcome adversaries (attacks)
- Need to understand
  - Who are the parties: context in which they act
  - What are the goals of the protocols
  - What are the capabilities of adversaries

Cryptographic protocols: Parties

- The good guys

Alice



Bob

Introduction of Alice and Bob attributed to the original RSA paper.

- The bad guys

Carl

Eve

Check out wikipedia for a longer list of malicious crypto players.

Cryptographic protocols: Objectives/Goals

- Most basic problem:
  - Ensure security of communication over an insecure medium
- Basic security goals:
  - **Confidentiality** (secrecy, confidentiality)
    - Only the intended recipient can see the communication
  - **Authenticity** (integrity)
    - Communication is generated by the alleged sender

Goals of modern cryptography

- Pseudo-random number generation
- Non-repudiation: digital signatures
- Anonymity
- Zero-knowledge proof
- E-voting
- Secret sharing

Cryptographic protocols: Attackers

- Interaction with data and protocol
  - Eavesdropping or actively participating in the protocol
- Resources:
  - Computation, storage
  - Limited or unlimited
- Access to previously encrypted communication
  - Only encrypted information (ciphertext)
  - Pairs of message and encrypted version (plaintext, ciphertext)
- Interaction with the cipher algorithm
  - Choose or not for what message to have the encrypted version (chose ciphertext)

Interaction with data and protocol

- Passive: the attacker only monitors the communication. It threatens confidentiality.
  - **Example**: listen to the communication between Alice and Bob, and if it's encrypted try to decrypt it.
- Active: the attacker is actively involved in the protocol in deleting, adding or modifying data. It threatens all security services.
  - **Example**: Alice sends Bob a message: 'meet me today at 5', Carl intercepts the message and modifies it 'meet me tomorrow at 5', and then sends it to Bob.

Resources

- In practice attackers have limited computational power
- Some theoretical models consider that the attacker has unlimited computational resources

Attacker knowledge of previous encryptions

- <u>Ciphertext-only attack</u>
  - Attacker knows only the ciphertext
  - A cipher that is not resilient to this attack is not secure
- <u>Known plaintext attack</u>
  - Attacker knows one or several pairs of ciphertext and the corresponding plaintext
  - Goal is to be able to decrypt other ciphertexts for which the plaintext is unknown

Interactions with cipher algorithm

- <u>Chosen-plaintext attack</u>
  - Attacker can choose a number of messages and obtain the ciphertexts for them
  - <u>*Adaptive*</u>: the choice of plaintext depends on the ciphertext received from previous requests
- <u>Chosen-ciphertext attack</u>
  - Similar to the chosen-plaintext attack, but the cryptanalyst can choose a number of ciphertexts and obtain the plaintexts
  - <u>*Adaptive*</u>: the choice of ciphertext may depend on the plaintext received from previous requests

What can we say about the adversary and the knowledge of the algorithm ? Should the algorithm be secret or not?

We will come back to this question.

Secret-key vs. public-key cryptography

- Secret-key cryptography (a.k.a. symmetric cryptography)
  - Encryption and decryption use the same key
  - Key must be kept secret
  - Key distribution is very difficult
- Public-key cryptography (a.k.a. asymmetric cryptography)
  - Encryption key different from decryption key
  - Cannot derive decryption key from encryption key
  - Higher cost than symmetric cryptography

Example based on symmetric key cryptographic protocols: GSM

GSM

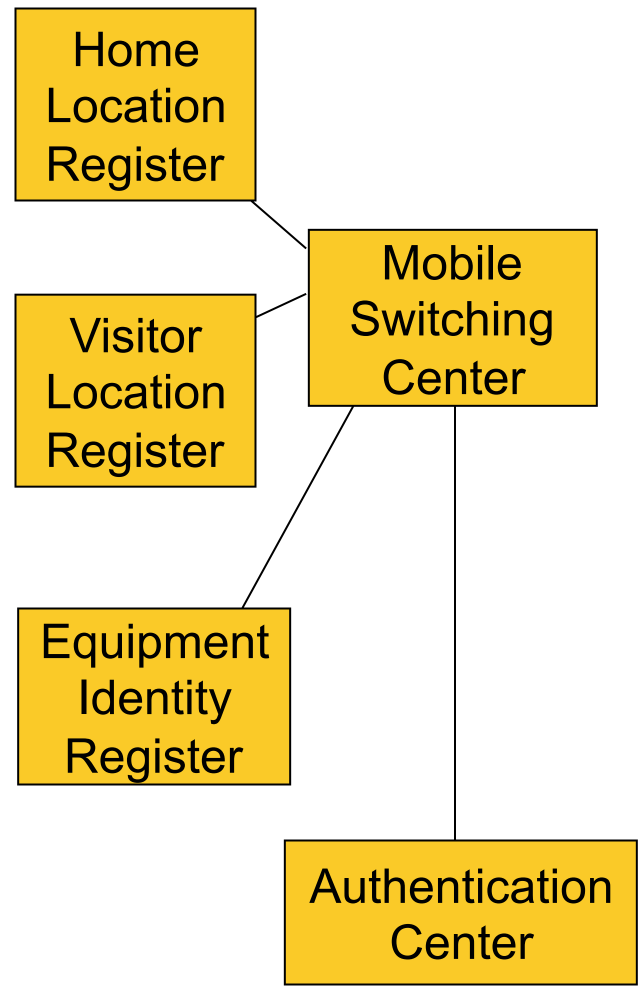
- Most popular cellular network
- Commercial operation began in 1991 with Radiolinja in Finland
- Four variants:
  - Most GSM networks operate in the 900 MHz or 1800 MHz bands.
  - United States and Canada use the 850 MHz and 1900 MHz bands because the 900 and 1800 MHz frequency bands were already allocated.
- Channel access mechanism is TDMA
- Several data services offered besides voice

GSM main security focus

- Focus:
  - Make sure the client is billed for the service
  - **Provide authentication, confidentiality and anonymity of the communication**
- Assumptions:
  - There is a long-term relationship between the client and the network operator (home network) in the form of a contract
  - The long-term relationship is represented by a long-term secret key shared by the client and network and serving as basis for authentication

Authentication architecture

- User is **permanently** associated with a home location register (HLR) in his subscribed network;
  - Contains user profile, billing and location information
- Visitor location register (VLR)
  - Maintains information about the roaming users; information is downloaded from the user's HLRs
- Authentication Center
  - Validates a user by verifying their identity with the Equipment Identity Register



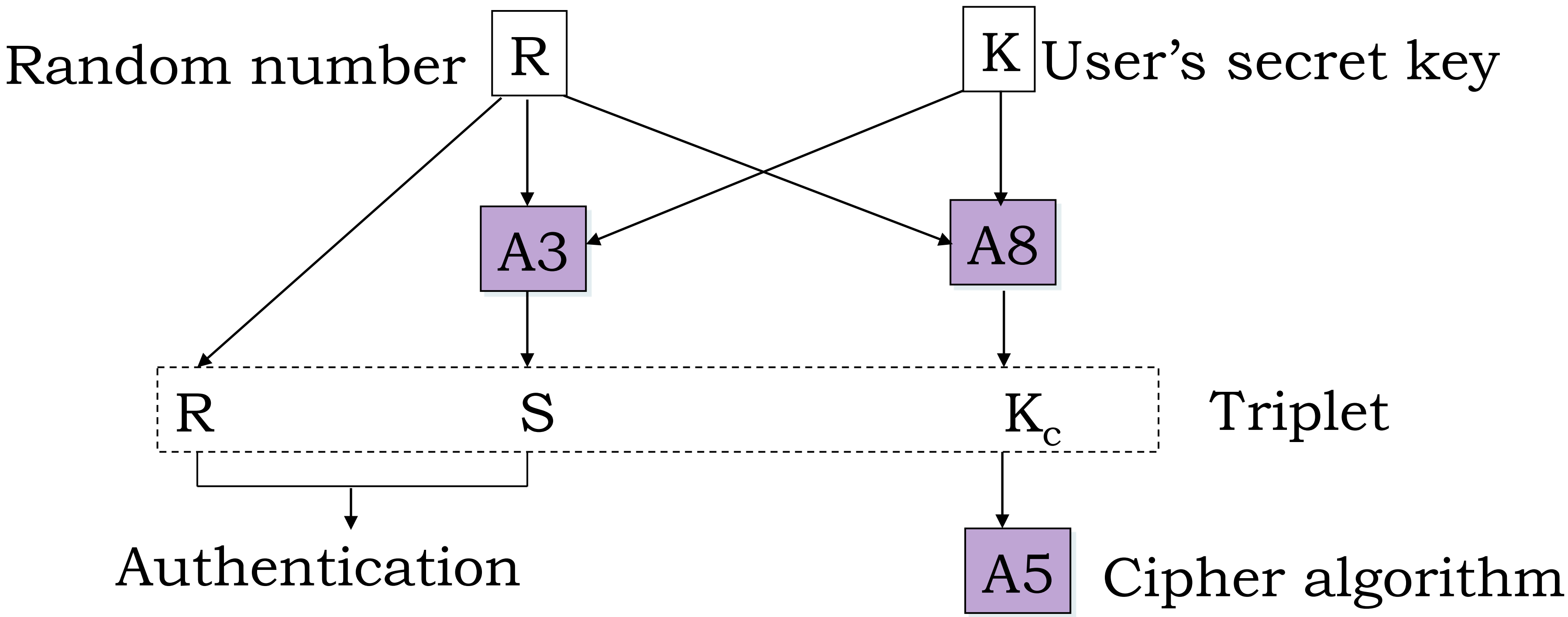
Subscriber Identity Module (SIM)

- Protected by a PIN code
- Removable from the terminal
- Contains all data specific to the end user which have to reside in the Mobile Station:
  - IMSI: International Mobile Subscriber Identity (permanent user's identity)
  - PIN
  - TMSI (Temporary Mobile Subscriber Identity)
  - K : User's secret key, long term
  - K_c : Ciphering (encryption) key
  - List of the last call attempts
  - List of preferred operators
  - Supplementary service data (abbreviated dialing, last short messages received,...)

GSM security goals

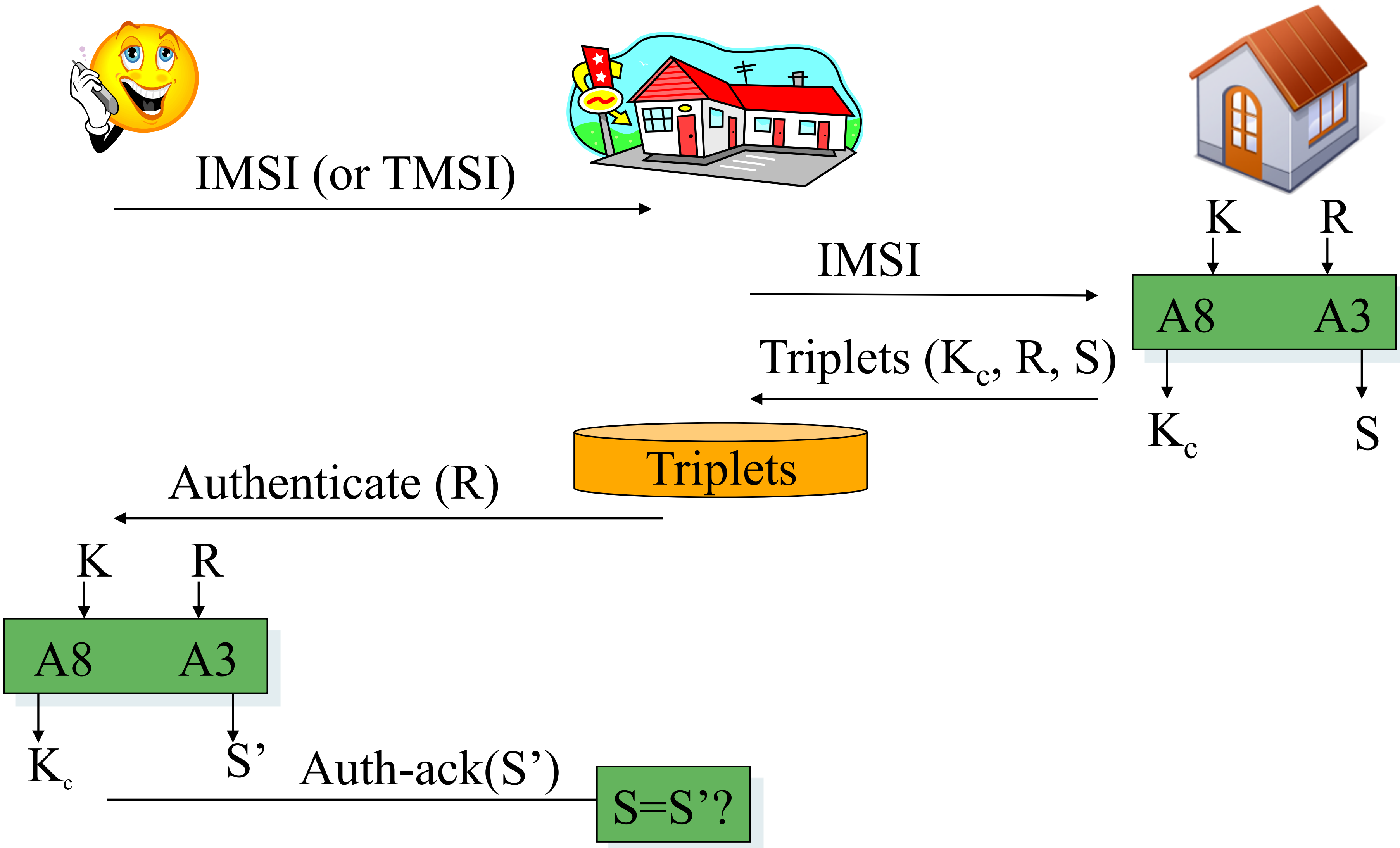
- **Authentication**: Subscriber authentication
  - challenge-response protocol
  - long-term secret key between subscriber and HLR
  - roaming without revealing long-term key to the VLR
- **Confidentiality**: Confidentiality of communications and signaling over wireless
  - key shared between the subscriber and VLR established with the help of HLR
- **Anonymity**: Protection of the subscriber's identity from eavesdroppers
  - usage of short-term temporary identifiers

Cryptographic algorithms of GSM



K_c: ciphering key
S : signed result
A3: subscriber authentication (operator-dependent algorithm)
A5: ciphering/deciphering (standardized algorithm)
A8: cipher generation (operator-dependent algorithm)

GSM authentication protocol

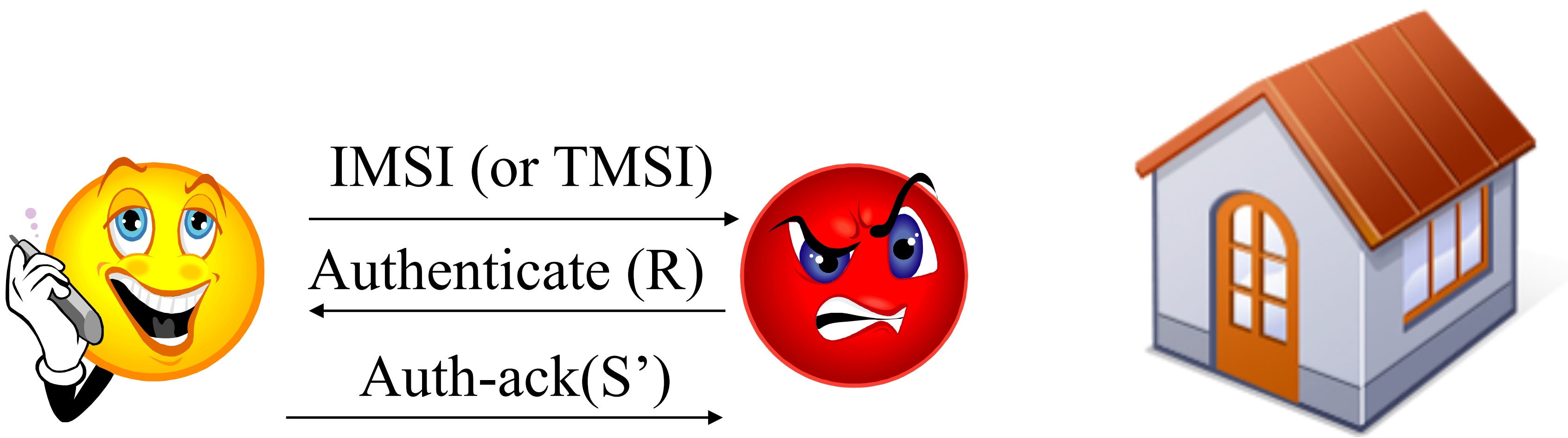


GSM anonymity

- **Temporary Mobile Subscriber Identity (TMSI)**: Client receives a temporary identification TMSI from VLR, encrypted with K_c
  - Stored in both the VLR database and on the mobile subscriber's SIM-card.
  - Valid for a VLR, in next authentication, the client can use the TMSI for authentication
  - If data context (the authentication triple) is no longer available, client needs to send the IMSI (start over)
- If the client moves into another visiting network, client contacts new VLR to obtain new TMSI

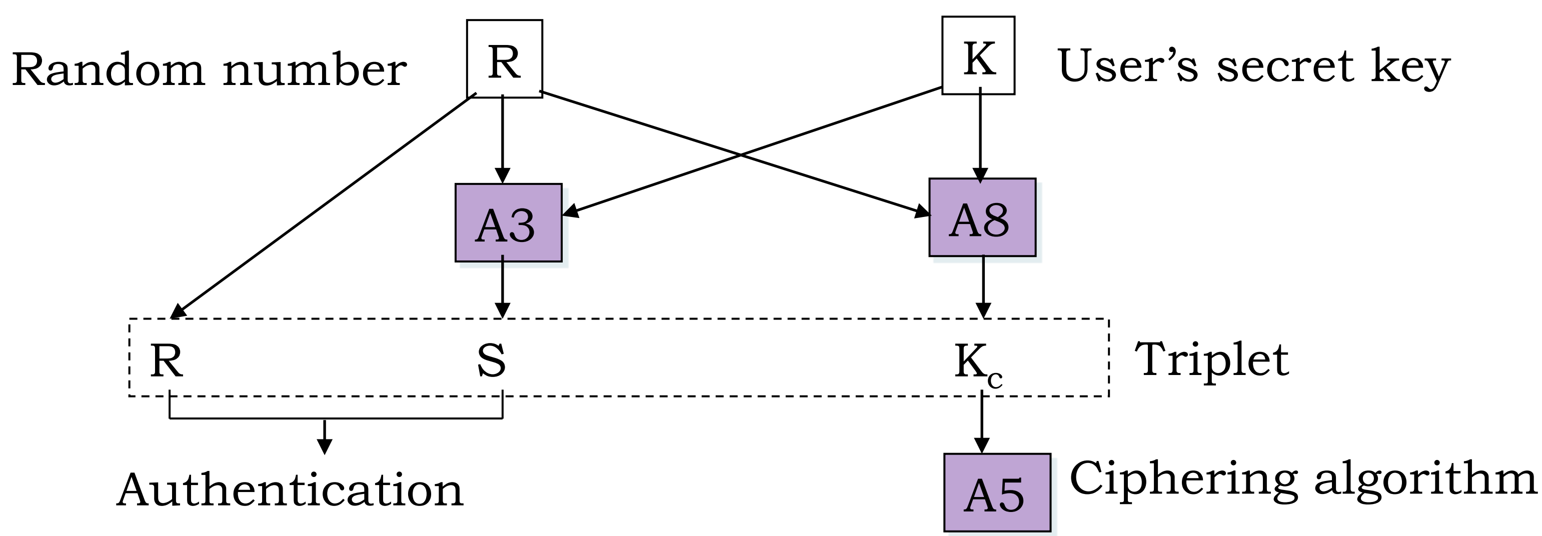
Impersonating the visiting network

- The visiting network is never authenticated, some entity can impersonate the visiting network
  - faked base stations attacks
  - technology exits, IMSI catcher



What if crypto algorithms are broken?

- If A5 broken – anybody can decipher communication
- If A3 broken – compute K based on S and R (which are sent on wireless by VLR and client)
- If A8 broken – compute K based on R and K_c



Attacks against A5/1

- Attacks against A5/1
  - Passive attacks: a number of attacks on A5/1 using known plaintext attacks.
  - Active attacks:
  - 2003 attacks using ciphertext-only
  - 2006 real-time decryption attacks demonstrated
  - 2009 Karsten Nohl announced that he had cracked the A5/1 cipher.
- Attacks against A3/A8
  - Several of them

Food for thought …

- Does secrecy of the algorithm provide “better” security?

- How do we know that a cryptographic algorithm is secure?

Kerchhoff's principle

The security of a protocol should rely only on the secrecy of the keys, protocol designs should be made public (1883)

- **security by obscurity does not work** (there are many examples, WEP, GSM, voting machines)

Dr Auguste Kerckhoff (19 January 1835 – 9 August 1903) was a Dutch linguist and cryptographer who was professor of languages at the School of Higher Commercial Studies in Paris in the late 19th century.

How do you know a cipher is secure?

- Show that under the considered attack model, security goals <u>are NOT achieved</u> (break it)
- Show that under the considered attack model, security goals <u>are achieved</u> (evaluate/prove)

Breaking ciphers…

- Different methods depending on:
  - Type of information available to the attacker
  - Interaction with the cipher machine
  - Computational power available to the attacker
- Attacks
  - Known plaintext
  - Known ciphertext
  - Chosen plaintext
  - Chosen ciphertext

Models for evaluating security

- **Unconditional (information-theoretic) security**
  - Adversary has unlimited computational resources
  - Plaintext and ciphertext modeled by their distribution, analysis is made by using probability theory
- **Provable security:**
  - Prove security properties based on assumptions that it is difficult to solve a well-known and supposedly difficult problem (example: computation of discrete logarithms, factoring)
- **Computational security (practical security)**
  - Measures the amount of computational effort required to defeat a system using the best-known attacks

Take home lessons

- Cryptographic protocols: parties, goals and attackers
- Symmetric cryptograph vs public-key cryptography
- Security should rely only on the secrecy of the key and not of the algorithm
- Security of ciphers: we break them or prove they achieve their goals under specific attacker models