Generic attacks on MAC schemes

Guessing the tag of a message $x \in \{0,1\}^*$.

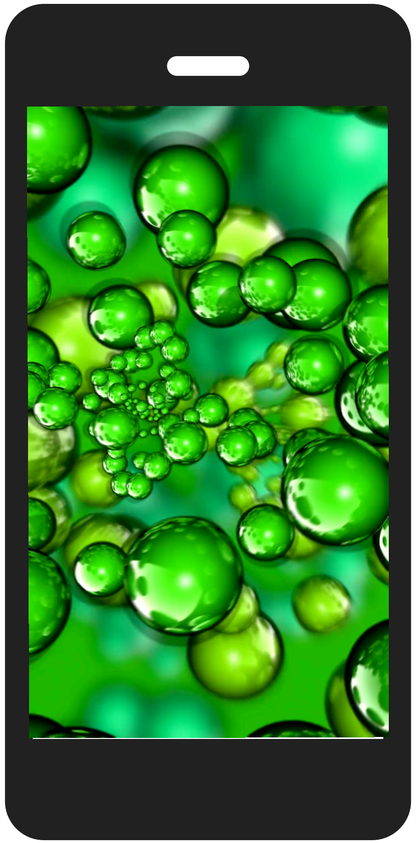
- **Attack**: Select $y \in_R \{0,1\}^n$ and guess that $\text{MAC}_k(x) = y$.
- **Analysis**: Assuming that the MAC scheme is ideal, the success probability is $1/2^n$.
- Note: Guesses cannot be directly checked.
- MAC tag guessing is infeasible if $n \geq 128$.

Generic attacks (2)

Exhaustive search on the key space:

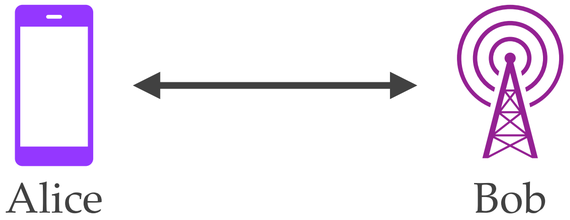
- **Attack**: Given r message-tag pairs $(x_1, t_1), \ldots, (x_r, t_r)$, one can check whether a guess h of the key is correct by verifying that $\mathrm{MAC}_h(x_i) = t_i$ for $i = 1,2,\ldots, r$.
- **Analysis**: Assuming that the MAC scheme is ideal, the expected number of keys for which all (x_i, t_i) pairs verify is $1 + FK = 1 + (2^\ell - 1)/2^{nr}$.
  For example, if $\ell = 128$, $n = 128$, $r = 2$, then $FK \approx 1/2^{128}$.
  Assuming that FK is negligible, the expected number of operations is $\approx 2^{\ell-1}$.
- Exhaustive key search is infeasible if $\ell \geq 128$.

GSM



- Global standards for mobile communications
  - 2G, 2.5G: GSM (Global System for Mobile Communications)
  - 3G: UMTS (Universal Mobile Telecommunications System)
  - 4G: LTE (Long Term Evolution)
  - 5G: NR (New Radio)
- We will *sketch* the basic security mechanism in GSM.
- GSM security is notable since it uses only symmetric-key primitives.
- 3G, 4G and 5G security improves upon GSM security in several ways, but will not be discussed here.

GSM security objectives



Objectives:

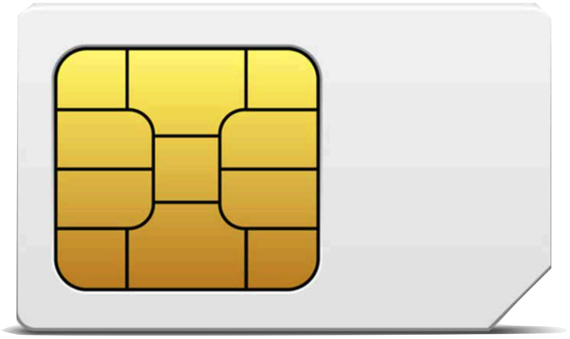
1. Entity authentication: The cell phone service provider needs the assurance that entities accessing its service are legitimate subscribers.

2. Confidentiality: The data exchanged between a cell phone user and their cell phone service provider should be confidential.

Note: GSM does *not* provide end-to-end security, i.e., confidentiality of the conversation between two cell phone users. Also, authentication is only one-way — the phone authenticates itself to the base station.

GSM description

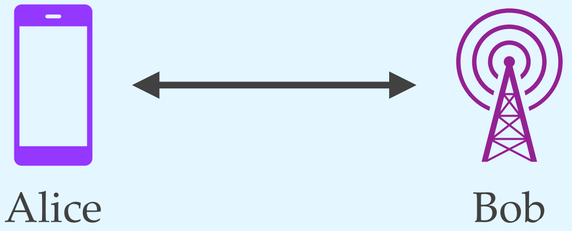
- **Cryptographic ingredients**:
  - Enc: A symmetric-key encryption scheme.
  - MAC: A symmetric-key MAC scheme.
  - KDF: A key derivation function.



- **Setup**:
  - A SIM card manufacturer (such as Gemalto) randomly selects a secret key k, and installs it in a SIM card. A copy of k is given to the cell phone service provider.
  - When a user subscribes to a cell phone service, she gets the SIM card which she installs in her phone.
  - Note: A different key k is chosen for each user.

GSM description (2)

Alice: cell phone user, Bob: cell phone service provider.



1. Alice sends an authentication request to Bob.
2. Bob selects a challenge $r \in_R \{0,1\}^{128}$ and sends r to Alice.
3. Alice's SIM card uses k to compute the response $t = \mathrm{MAC}_k(r)$.
   Alice sends t to Bob.
4. Bob retrieves Alice's key k from its database, and verifies that $t = \mathrm{MAC}_k(r)$.
5. Alice and Bob compute an encryption key $K_E = \mathrm{KDF}_k(r)$, and thereafter use the encryption algorithm $\mathrm{Enc}_{K_E}(\cdot)$ to encrypt and decrypt messages for each other for the remainder of the session.