Kryptografia w sieci komórkowej

Rafał Leja

9 luty 2026

Standardy sieci komórkowych

1G - Początki

NTT, Nippon Telegraph and Telephone - **1979**, **Japonia**

NMT, Nordic Mobile Telephone - **1981**, **Skandynawia**

AMPS, Advanced Mobile Phone System - **1983**, **USA**

1G

- **Analogowe** systemy telefonii komórkowej
- **Tylko głos**, brak transmisji danych
- **Brak szyfrowania**, podatność na podsłuch

2G - Cyfrowa rewolucja

GSM, Global System for Mobile Communications - **1991**, **Europa**

CDMA, Code Division Multiple Access - **1995**, **USA**

PDC, Personal Digital Cellular - **1993**, **Japonia**

2G

- **Cyfrowe** systemy telefonii komórkowej
- Wprowadzenie **transmisji danych** (SMS, MMS)
- **Szyfrowanie**:
  - A5/1 - silne szyfrowanie, używane w Europie
  - A5/2 - słabsze, eksportowe szyfrowanie
  - A5/3 (KASUMI) - ulepszona wersja, stosowana w późniejszych implementacjach GSM

3G - Era multimediów

UMTS, Universal Mobile Telecommunications System - **2001**, Europa

CDMA2000 - 2000, USA

HSPA/HSPA+ - 2005/2007, Globalnie

3G

- **Szybsze prędkości transmisji danych** (384 Kbps / 42 Mbps)
- Obsługa **multimediów** (wideo, VoIP)
- Ulepszone **szyfrowanie**:
  - KASUMI - używany w UMTS, oparty na A5/3
  - SNOW 3G - używany w CDMA2000, oparty na SNOW 2.0
- **Integralność** danych i **uwierzytelnianie** użytkowników

4G - Era LTE

LTE, Long Term Evolution - **2009**, **Globalnie**

WiMAX - **2007**, **Globalnie**

4G

- Standard **IP** dla transmisji danych i głosu (**VoLTE**)
- **Bardzo szybkie** prędkości transmisji danych (100 Mbps / 1 Gbps)
- Obsługa **zaawansowanych multimediów** (HD wideo, gry online)
- Zaawansowane **szyfrowanie**:
  - AES - używany w LTE, oparty na standardzie AES
  - SNOW 3G - kontynuacja użycia z 3G
- Ulepszone **uwierzytelnianie** i **integralność** danych

5G - Era łączności masowej

5G NR, New Radio - 2019, Globalnie

5G mmWave - 2019, Globalnie

5G

- Jeszcze szybsze prędkości (**10 Gbps** / **20 Gbps**)
- Bardzo niskie opóźnienia (**1 ms**)
- Obsługa **masowej łączności** (IoT, mMTC)
- Szyfrowanie i bezpieczeństwo:
  - AES-256 - wzmocnione szyfrowanie dla 5G
  - ZUC - algorytm strumieniowy używany w 5G, oparty na ZUC-128
  - **SUCI** zamiast IMSI

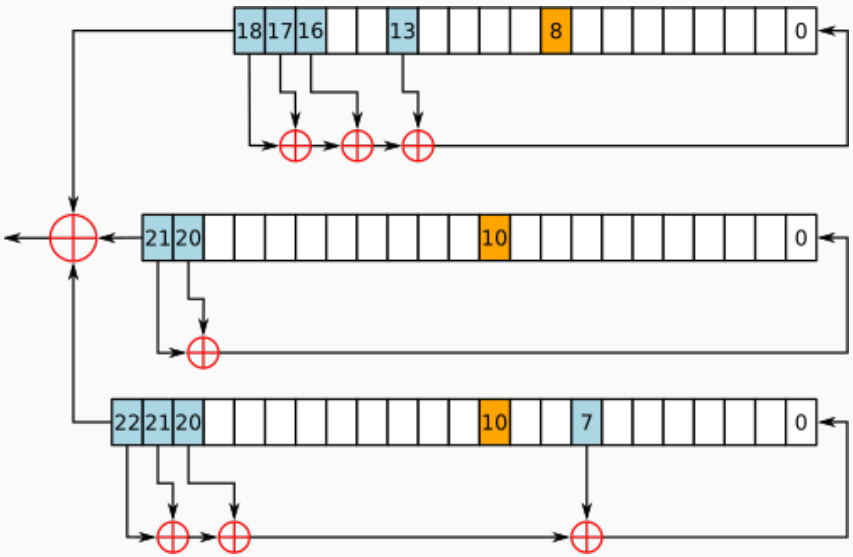
Podatności

Podatności

- Złamanie A5/1
- Downgrade Attack
- IMSI Catcher (Stingray)

Budowa A5/1

- Oparty na trzech rejestrach przesuwających (LFSR)
- IV:
  - 64 bity klucza
  - 22 bity numeru ramki
- Stan: 19 + 22 + 23 = 64 bity
- Keystream: 2*114 bitów



Złamanie A5/1

Offline:

- Mamy 2^{64+22} możliwych kluczy

Złamanie A5/1

Offline:

- Mamy 2^{64+22} możliwych kluczy
- Ale tylko 2^{64} możliwych stanów (tak naprawdę $2^{61.16}$)

Złamanie A5/1

Offline:

- Mamy 2^{64+22} możliwych kluczy
- Ale tylko 2^{64} możliwych stanów (tak naprawdę $2^{61.16}$)
- Zamiast pamiętać 2^{64} stanów, używamy **Rainbow Tables**

Złamanie A5/1

Offline:

- Mamy 2^{64+22} możliwych kluczy
- Ale tylko 2^{64} możliwych stanów (tak naprawdę $2^{61.16}$)
- Zamiast pamiętać 2^{64} stanów, używamy **Rainbow Tables**

Online:

- Przechwytujemy szyfrogram
- Odzyskujemy keystream dzięki znanym tekstom jawnym (np. nagłówkom)
- Przeszukujemy Rainbow Tables, aby znaleźć odpowiadający stan i klucz

Downgrade Attack

- Stawiamy fałszywą **stację bazową**, która jest silniejsza od prawdziwej
- Obsługujemy tylko **2G** oraz **A5/2** (A5/1 z krótszym kluczem)

IMSI Catcher (Stingray)

- Urządzenie podszywające się pod stację bazową (około $100k)
- Pozyskuje **IMSI** (International Mobile Subscriber Identity)
- Oraz **IMEI** (International Mobile Equipment Identity)

Zastosowania IMSI Catcher

- **Identyfikacja** osób
- **Śledzenie** i **lokalizacja** użytkowników
- W niektórych przypadkach **podsłuchiwanie** rozmów i wiadomości

Zabezpieczenia

Zabezpieczenia

- Wyłączenie **2G** i wymuszenie **4G/5G**

Zabezpieczenia

- Wyłączenie **2G** i wymuszenie **4G/5G**
- Detekcja **IMSI Catcherów** (np. Rayhunter)

Zabezpieczenia

- Wyłączenie **2G** i wymuszenie **4G/5G**
- Detekcja **IMSI Catcherów** (np. Rayhunter)
- Szyfrowanie end-to-end (E2EE)

Zabezpieczenia

- Wyłączenie **2G** i wymuszenie **4G/5G**
- Detekcja **IMSI Catcherów** (np. Rayhunter)
- Szyfrowanie end-to-end (E2EE)
- Nieużywanie SMS do **2FA**

Źródła

Wikipedia:

- `{1..5}`G
- Stingray phone tracker
- A5/1