Chameleon Ultra v2.0



Chameleon Ultra v2.0 — це компактний бездротовий **RFID/NFC-емулятор, зчитувач та дублікатор** «3-в-1» з відкритим вихідним кодом. Пристрій розроблено спільнотою RfidResearchGroup для інженерів СКУД, фахівців із кібербезпеки (пентестерів) та RFID-ентузіастів. Головне завдання девайса — об'єднати до 16 фізичних перепусток і ключів в одному кишеньковому брелоку

Ключові можливості

Двочастотний режим: Працює одночасно на низькій частоті **LF (125 кГц)** та високій частоті **HF (13.56 МГц)**
Велика пам'ять: Має **8 незалежних слотів**. Кожен слот може зберігати по одному LF та одному HF ключу (загалом до 16 міток)
Повна емуляція та запис: Здатний зчитувати, зберігати та емолювати картки в реальному часі, а також записувати копії на сторонні карти-болванки
Керування по Bluetooth: Завдяки BLE-модулю девайс миттєво підключається до фірмового застосунку **Chameleon Ultra GUI** на смартфонах (Android, iOS) та ПК (Windows, macOS, Linux)

Підтримувані формати карт

- **Низькочастотні (125 кГц)**: EM4100, T5577, HID ProxCard II тощо.
- **Високочастотні (13.56 МГц)**: MIFARE Classic (з підтримкою розшифровки та атак на вразливості), MIFARE Ultralight, NTAG та інші карти стандарту ISO 14443A/B. *Захищені картки на кшталт MIFARE DESFire або банківські чипи копіюванню не підлягають*

Технічні характеристики та версія v2.0

- **Габарити**: Ультракомпактний формат (45 x 25 x 7 мм), вага всього 10 грамів.

- **Живлення**: Вбудований акумулятор на 500 мАг, зарядка через сучасний **USB Type-C**. Заряду вистачає на кілька тижнів автономної роботи.
- **Особливості v2.0**: Версія 2.0 отримала оптимізовану схемотехніку антен, прозору кришку корпусу з чіткою LED-індикацією слотів, а також **функцію швидкого апаратного перезавантаження** подвійним натисканням кнопок на випадок збою чи зависання під час тестування

Управління на корпусі здійснюється лише двома кнопками (A і B). Коротким натисканням ви перемикаєте слоти карт доступу, довгим утриманням A — копіюєте UID мітки, а довгим утриманням B — перевіряєте рівень заряду батареї за шкалою світлодіодів

Проблема з розшифровкою ключа зазвичай виникає через те, що картка має **високий рівень захисту**, **унікальні зашифровані сектори** (Hardened MIFARE), або є **динамічною** (наприклад, MIFARE DESFire). Chameleon Ultra v2.0 має потужний функціонал для обходу базових систем захисту, але деякі типи міток вимагають специфічного підходу.

4 головні причини, чому Chameleon не розшифровує ключ:

1. **Це мітка MIFARE Classic із виправленою вразливістю (Hardened)**
   Старі атаки типу *Nested* або *Darkside* не працюють на нових ревізіях карток, де виправлено генератор випадкових чисел (PRNG). Для них потрібна сучасна атака **Hardnested**.
2. **У зчитувача та картки немає спільних відомих ключів (Nonces)**
   Якщо в базі даних додатка Chameleon Ultra GUI немає жодного правильного ключа від секторів цієї карти, девайс не зможе зачепитися за шифрування (так звана проблема "Zero Known Keys").
3. **Це картка надвисокої безпеки (DESFire / Plus / iCLASS)**
   Chameleon Ultra **не вміє і не зможе** розшифрувати картки MIFARE DESFire, Plus (у режимі SL3) або HID iCLASS. Вони використовують сучасне шифрування AES/DES, яке наразі неможливо зламати перебором чи атаками на радіоінтерфейс.
4. **Нестабільне положення антени (Bad Alignment)**
   Антени в Chameleon Ultra v2.0 дуже компактні. Якщо під час розрахунку ключів картку трохи посунути, процес зчитування та збору криптографічних відповідей (nonces) перерветься помилкою.

Покрокова інструкція: як зняти ключі та розшифрувати карту

Виконайте ці кроки послідовно через офіційний комп'ютерний або мобільний додаток **Chameleon Ultra GUI**:

1. Оновіть словники ключів (Key Dictionaries)

Перед скануванням переконайтеся, що додаток використовує розширену базу стандартних ключів.

- Перейдіть у меню **Settings** або **Keys Management**.
- Завантажте або активуйте **System Dictionary** (зазвичай містить понад 2000 поширених заводських ключів). Досить часто хоча б один сектор відкривається стандартним ключем, що відкриває шлях до повної розшифровки.

2. Запустіть правильний тип атаки

Замість швидкого сканування скористайтеся розширеними утилітами Crypto у додатку:

- Спробуйте запустити **Mifare Classic nested attack**, якщо додаток знайшов бодай один правильний ключ (зелений сектор).
- Якщо картка сучасна та захищена, оберіть **Hardnested attack**. Пристрій почне збирати тисячі криптографічних відповідей від карти. Цей процес може тривати від 5 до 30 хвилин. **Важливо:** тримайте карту нерухомо впритул до антени Chameleon протягом усього часу.
3. Використайте атаку "Reader Attack" (Sniffing)

Якщо картка взагалі не піддається розшифровці напряму (немає жодного відомого ключа), вам потрібно перехопити ключ у момент, коли карту прикладають до реального зчитувача (наприклад, на дверях під'їзду чи турнікеті):

1. Увімкніть у додатку режим **Sniffing** (перехоплення) для потрібного слоту.
2. Піднесіть Chameleon Ultra до **реального настінного зчитувача/домофона**.
3. Прикладіть оригінальну карту до Chameleon. Пристрій перехопить легітимний обмін даними та законний ключ, який зчитувач надсилає картці.
4. Підключіть девайс до додатка та розшифруйте решту секторів за допомогою знайденого ключа.

Словники,

Щоб розширити словники ключів (Key Dictionaries) у Chameleon Ultra та підвищити шанси на злам мітки, вам потрібно завантажити готові бази ключів з інтернету та імпортувати їх у додаток **Chameleon Ultra GUI** (або Chameleon Ultra App на телефоні).

Ось найефективніші способи, як це зробити.

Спосіб 1. Автоматичне скачування найбільших баз (Рекомендовано)

У спільноті RFID є готові списки, які містять мільйони відомих ключів від китайських домофонів, СКУД Vizit, Cyfral, Metakom та офісних перепусток.

1. Відкрийте додаток **Chameleon Ultra GUI** на ПК або смартфоні.
2. Перейдіть у розділ **Dictionaries** (або **Keys / Key Management**).
3. Знайдіть кнопку **Download from URL** (або **Import from Web**).
4. Вставте туди посилання на один із відомих Github-репозиторіїв з великими словниками (наприклад, словники від Proxmark3 або Flipper Zero) та натисніть «Завантажити».
💡 *Порада: Найпопулярніший та найбільший словник у світі RFID — це* `mifare_default.dic` *від проекту Proxmark3. Він містить тисячі стандартних комбінацій.*

Спосіб 2. Ручне створення та імпорт свого словника

Якщо ви знайшли ключі на форумах або знаєте специфічні коди вашого міста/провайдера домофонів, ви можете створити власний словник:

1. Відкрийте звичайний **Блокнот** (на ПК) або будь-який текстовий редактор на телефоні.

2. Впишіть туди ключі у 16-ричному форматі (HEX), кожен ключ — **з нового рядка**. Вони мають складатися рівно з 12 символів (6 байт).

   Приклад текстового файлу:

   text
   ```
   FFFFFFFFFFFF
   A0A1A2A3A4A5
   B0B1B2B3B4B5
   000000000000
   4D3A99C351DD
   ```
   Будьте обачні, використовуючи код.

3. Збережіть файл під назвою, наприклад, `my_keys.dic` або `custom.txt`.
4. У додатку Chameleon натисніть **Import File** (або **Upload Dictionary**) та виберіть створений файл.

Спосіб 3. Копіювання словників від Flipper Zero

Якщо у вас чи ваших знайомих є мультитул Flipper Zero, його словник MIFARE є одним із найкращих для країн СНД та Європи, оскільки він постійно оновлюється спільнотою.

1. Завантажте на ПК офіційний репозиторій словників Flipper Zero (файл `nfc_dict.txt`).
2. Очистіть його від зайвих коментарів (якщо вони є) та залиште лише чисті 12-символьні HEX-коди.
3. Імпортуйте цей текстовий файл у Chameleon Ultra GUI через кнопку **Import**.

Що робити після розширення словника?

Коли додаток покаже, що у вашій базі тепер не 10-20 ключів, а кілька тисяч:

1. Знову прикладіть картку до Chameleon Ultra.
2. Запустіть функцію **Dictionary Attack** (або **Check Default Keys**).
3. Додаток почне перебирати всі завантажені ключі по черзі. Це займе трохи більше часу, але якщо знайдеться хоча б один збіг (хоча б для сектора 0 чи будь-якого іншого) — сектор підсвітиться **зеленим**.
4. Після цього одразу запускайте атаку **Nested Attack**. Використовуючи цей один знайдений ключ як «зачіпку», Chameleon зможе математично розрахувати ключі до всіх інших закритих секторів картки за кілька хвилин.