

# **Bezpieczeństwo kart elektronicznych**

**Krzysztof Maćkowiak**

Karty elektroniczne wprowadzane od drugiej połowy lat 70-tych znalazły szerokie zastosowanie w wielu dziedzinach naszego życia:

- bankowości,
- telekomunikacji,
- handlu,
- sieciach GSM (karty SIM),
- szkolnictwie,
- płatnych usługach TV (dekodery telewizji kablowej),
- służbie zdrowia,
- systemach ubezpieczeń,
- systemach opieki społecznej,
- komunikacji i transporcie.

Dzięki usługom kryptograficznym używane są w celu uwierzytelnienia oraz autoryzacji w przedsiębiorstwach, instytucjach, ich sieciach komputerowych oraz VPN. Mogą być również stosowane do składania podpisów elektronicznych.

W celu bezpiecznego przechowywania i przesyłania danych w kartach elektronicznych wykorzystuje się znane algorytmy kryptograficzne. Złożoność tych algorytmów spowodowała wprowadzenie do kart elektronicznych dodatkowych koprocessorów, zwiększających szybkość wykonywania operacji arytmetycznych. W wielu przypadkach wpłynęło to na zmniejszenie dostępnej pamięci, ze względu na określone rozmiary kart elektronicznych. Pamięć EEPROM w kartach kryptograficznych wynosi od 8 do 64 kB. Z biegiem czasu wprowadzane są coraz szybsze koprocessory. Przykładowe koprocessory firmy Philips: CORSAIR, FAME, FAMEX.

W kartach elektronicznych stosuje się zarówno algorytmy szyfrowania symetrycznego, jak również szyfrowania asymetrycznego, algorytmy podpisu cyfrowego oraz funkcje skrótu.

Algorytm symetryczny DES jako pierwszy został zaimplementowany w roku 1985 w kartach firmy Philips. W roku 1991 zaimplementowano algorytm szyfrowania asymetrycznego.

Najpopularniejsze algorytmy kryptograficzne stosowane w kartach elektronicznych:

- szyfrowanie symetryczne
  - DES,
  - 3DES
  - IDEA,
- szyfrowanie asymetryczne
  - RSA,
  - ECC,
- podpis cyfrowy
  - RSA,
  - ECDSA,
- uzgadnianie klucza
  - Diffie-Hellman,
- funkcje skrótu
  - SHA,
  - MD5.

Najnowszy standard szyfrowania symetrycznego AES również znakomicie nadaje się do implementacji na kartach.

W wielu kartach algorytmy kryptograficzne m.in. algorytmy DES i RSA realizowane są sprzętowo w celu przyspieszenia obliczeń. W przypadku

korzystania z algorytmów asymetrycznych stosuje się funkcje skrótu: MD5, SHA-1.

Korzystając z koprocatora FAMEX możliwe jest generowanie podpisu cyfrowego z wykorzystaniem algorytmu RSA z kluczem 1024 bitowym w czasie  $\leq 160\text{ms}$  i jego weryfikacji w czasie  $\leq 400\text{ms}$ .

W przypadku kart Philips z rodziny MIFARE szyfrowanie odbywa się z użyciem realizowanego sprzętowo potrójnego algorytmu DES (3DES). Czas wykonywania operacji szyfrowania w przypadku tych kart wynosi  $5\mu\text{s}$ .

Dzięki zastosowaniu silnych algorytmów kryptograficznych karty elektroniczne stanowią bezpieczny nośnik informacji, kluczy kryptograficznych, umożliwiają szyfrowanie oraz deszyfrowanie danych, uwierzytelnienie z wykorzystaniem protokołu obustronnego uwierzytelniania (ISO 9798-2), składanie podpisów elektronicznych.

W kartach elektronicznych stosuje się również struktury odpowiadające generatorom pseudolosowym. Oparte są one na algorytmach deterministycznych a losowe ziarno pobierane jest z pamięci nieulotnej lub przesyłane ze świata zewnętrznego. Bardziej zaawansowane rozwiązania wykorzystują m.in. naturalne szумы cieplne struktur krzemowych.

W celu uwierzytelnienia użytkownika karty stosuje się hasła, PINy lub metody biometryczne.

Sama karta oraz układy scalone muszą być również zabezpieczone. Przed wprowadzeniem karty na każdym etapie cyklu jej życia przeprowadzane są testy, sprawdzające niezawodność karty. Dodatkowo ze względu na ochronę przed atakami na układ scalony muszą być spełnione następujące warunki:

- układ poddawany zakłóceniom zewnętrznym może ulec zniszczeniu, lecz nie może umożliwić odczytania ani zmodyfikowania przechowywanych danych,
- każda próba rozpoznania lub przeanalizowania wewnętrznej struktury układu prowadzi do jego nieodwracalnego zniszczenia (czujniki uaktywniające mechanizmy destrukcyjne karty).

Karty elektroniczne umożliwiają zapisanie 8-16 kluczy, które zwiększają bezpieczeństwo na poszczególnych etapach cyklu życia karty: producent-dostawca-użytkownik.

Dodatkowo na kartach wprowadzone pewne zewnętrzne zabezpieczenia takie jak: numer karty, dane, zdjęcie oraz podpis właściciela, okres ważności karty oraz hologram.

Elementy bezpieczeństwa muszą być zastosowane w całym cyklu życia karty, od jej wyprodukowania, poprzez jej wydanie, użytkowanie i po tym czasie. Ważnym elementem jest nadzorowanie produkcji i transportu kart.

Należy pamiętać również o bezpieczeństwie czujników i systemów wykorzystujących karty elektroniczne.

### **Algorytmy kryptograficzne stosowane w kartach SIM**

W kartach SIM wykorzystywanych w systemach GSM stosuje się następujące algorytmy:

- algorytm A3 – uwierzytelnianie tożsamości w trybie wyzwanie-odpowiedź,
- algorytm A8 – generowanie i poufne przesyłanie klucza sesyjnego,
- algorytm A5 – szyfrowanie strumieniowe przesyłanych informacji zakodowanych cyfrowo oraz sygnałów sterujących sesją łączności.

Algorytmy A3 i A8 występują najczęściej jako jeden symetryczny blokowy algorytm szyfrowania połączony z funkcją jednokierunkową i noszący nazwę COMP128.

Algorytm A5 oparty jest na trzech rejestrach liniowych ze sprzężeniem zwrotnym (LFSR), inicjowanych na podstawie 64-bitowego jednorazowego tajnego klucza sesyjnego oraz 22-bitowego klucza jawnego. Wyróżniamy algorytmy A5/1 oraz A5/2. Algorytm A5/1, mimo że jest silniejszy od algorytmu A5/2, może być złamany w czasie rzeczywistym. Udana kryptoanaliza przeprowadzona została przez Birjukow'a i Shamir'a. Wadą tego algorytmu jest wykorzystanie klucza sesyjnego o długości 54 bitów, uzupełnionego o 10 bitów zerowych, co upraszcza kryptoanalizę.

W kartach elektronicznych wprowadzonych przez firmę BULL korzysta się z algorytmu szyfrowania symetrycznego DES lub tajnego algorytmu TELEPASS. Zapewniają one uwierzytelnianie oraz poufność przesyłanych sekretów.

### **Standardy związane z bezpieczeństwem kart elektronicznych:**

- ISO/IEC 7816-8, *Security related interindustry commands*.
- ISO/IEC 7816-9, *Additional interindustry commands and security attributes*.
- ISO 10202-1, *Financial transaction cards – Security architecture of financial systems using integrated circuit cards – Card life cycle*.
- ISO 10202-3, *Financial transaction cards – Security architecture of financial systems using integrated circuit cards – Cryptographic key relationships*.
- GSM 03.48, *Digital cellular telecommunications system; Security mechanism for the SIM application toolkit*.
- FIPS 140-1, *Security Requirements for Cryptographic Modules*.

### **Literatura**

1. Kubas Monika, Molski Marian, *Karta elektroniczna. Bezpieczny nośnik informacji*. MIKOM 2002.
2. Chocianowicz Włodzimierz, Urbanowicz Jerzy, *Kryptografia w kartach elektronicznych: możliwości i ograniczenia*.