

NSA ujawnia stare szyfry

<http://ipsec.pl/nsa-ujawnia-stare-szyfry.html>

Amerykańska agencja NSA ujawniła dziewięć nowych dokumentów z lat 1977-98. Dotyczą one różnych opracowanych przez NSA technik kryptograficznych i wcześniej były zastrzeżone jako tajne lub ściśle tajne.

Najstarszy dokument to praca "The Authentication Problem" Jamesa H. Ellisa z 1977 roku podsumowująca wcześniejsze prowadzone wewnątrz NSA i GCHQ dyskusje na temat algorytmu NSE ("Non-Secret Encryption"), który w tym samym roku został niezależnie odkryty przez Rivesta, Shamira i Adlemana i nazwany RSA. Dyskusje te były prowadzone między Ellisem, Cliffordem Cocksem i Malcolmem Williamsonem od początku lat 70-tych i dziś tych trzech badaczy uznaje się za pionierów kryptografii z kluczem publicznym, choć świat dowiedział się o ich odkryciach dopiero w 1997 roku, a oryginalne publikacje z tamtych lat zostały ujawnione w większej partii dopiero teraz.

Odtajnione przez NSA dokumenty mają dziś wartość głównie historyczną, choć pojawia się tam także kilka algorytmów z lat 90-tych. Pokazują one jednak w jaki sposób myśleli trzydzieści lat temu badacze i przed jakimi problemami stawali - np. Ellis sporo wysiłku włożył w wyjaśnienie w swoim dokumencie jak to jest możliwe, że używany do szyfrowania klucz może być ujawniony bez utraty poufności kryptogramu?

W innym dokumencie dowiadujemy się, że w 1993 roku NSA szykowała dla nas alternatywną, "modularną" wersję PKI z funkcjonalnością "depozytu klucza" ("key escrow"). Pomysłów tych administracja amerykańska twardo trzymała się do roku 2000, kiedy ostatecznie zliberalizowano amerykańskie przepisy eksportowe i porzucono idee dopuszczenia do użytku tylko jednego "państwowego" szyfru (SKIPJACK).

Źródło: <http://cryptome.org/nsa-nse/nsa-nse-01.htm> "NSA Releases Top Secret Crypto Papers", Cryptome, 3. marca 2007