Summaries

Natalia Krzyworzeka: **Asymmetric cryptography and trapdoor one-way functions** • Automatyka/ Automatics 2016, Vol. 20, No. 2

The asymmetric-key (public-key) encryption scheme is considered to be the most important discovery in the history of cryptography. It is based on the use of two complementary keys generated according to a chosen trapdoor one-way function (TOWF). Since its first implementation, asymmetric encryption has revolutionized our way of communicating as well as the safety of information transfer, and it is now widely used around the world for various purposes, especially in the field of online transaction security.

The safety of the asymmetric-key scheme relies on the assumption that any known cryptographic attack using an efficient problem-solving algorithm will not be able to succeed in applying the inverse (decryption) function onto the cryptogram in a polynomial time without additional knowledge (secret information). The most-challenging aspect of creating a new asymmetric cryptographic algorithm is selecting a one-way function for encryption purposes and finding a trapdoor in its inverse. In this paper, the concept of public-key cryptography will be explained using the RSA algorithm as an example. In addition, the review of the most-important functions that are considered to be trapdoor one--way functions will be conducted.

Keywords: *cryptography, RSA algorithm, one-way function, one-way trapdoor function, public-key encryption, asymmetric encryption*

Streszczenia

Natalia Krzyworzeka: **Kryptografia asymetryczna i funkcje jednokierunkowe** • Automatyka/ Automatics 2016, Vol. 20, No. 2

Odkrycie szyfrowania asymetrycznego jest uważane za największy przełom w dziedzinie kryptografii. W założeniu kryptografia asymetryczna polega na generowaniu dwóch komplementarnych

kluczy według wybranej jednokierunkowej funkcji zapadkowej (*trapdoor one-way function*). Odkrycie tego sposobu szyfrowania całkowicie zrewolucjonizowało metody bezpiecznego przesyłu informacji i jest obecnie wykorzystywane w wielu dziedzinach, szczególnie przy uwierzytelnianiu danych oraz w transakcjach online.

Skuteczność omawianej metody pozwala założyć, że żaden algorytm deszyfrujący działający w realnym czasie nie będzie w stanie bez dodatkowych informacji (tzw. zapadki) efektywnie odgadnąć funkcji deszyfrującej. Największym utrudnieniem przy tworzeniu nowego algorytmu asymetrycznego jest odkrycie nowej, jednokierunkowej funkcji zapadkowej. W poniższym artykule zostanie dokładnie opisane działanie najbardziej znanego algorytmu asymetrycznego – RSA. Przeprowadzono również przegląd najważniejszych funkcji jednokierunkowych.

Słowa kluczowe: *kryptografia, algorytm RSA, funkcja jednokierunkowa, jednokierunkowa funkcja zapadkowa, klucz publiczny, kryptografia asymetryczna*