Kryptografia z kluczem publicznym

Kryptografia – nauka o przekazywaniu informacji w sposób zabezpieczony przed niepowołanym dostępem.

Podział kryptografii:

a) kryptografia symetryczna
b) kryptografia asymetryczna

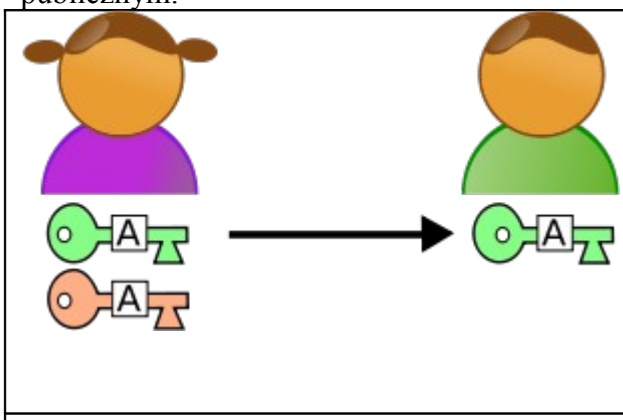
Kryptografia symetryczna to taki rodzaj szyfrowania, w którym tekst jawny ulega przekształceniu na tekst zaszyfrowany za pomocą pewnego klucza, a do odszyfrowania jest niezbędna znajomość tego samego klucza.

Kryptografia asymetryczna to rodzaj kryptografii, w którym używa się zestawów dwu lub więcej powiązanych ze sobą kluczy, umożliwiających wykonywanie różnych czynności kryptograficznych.

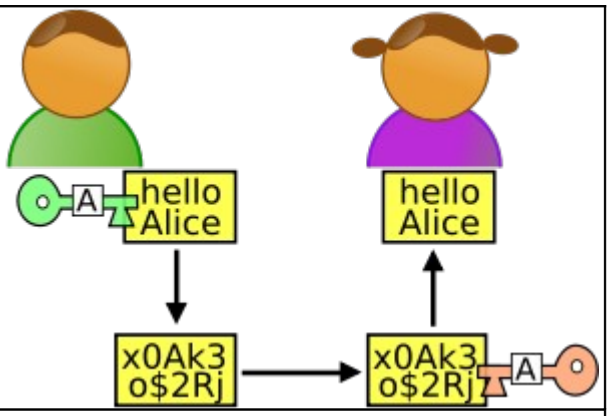
Najważniejsze zastosowania kryptografii asymetrycznej – szyfrowanie i podpisy cyfrowe – zakładają istnienie 2 kluczy – prywatnego i publicznego, przy czym klucza prywatnego nie da się łatwo odtworzyć na podstawie publicznego.

Klucz publiczny używany jest do zaszyfrowania informacji, klucz prywatny do jej odczytu. Ponieważ klucz prywatny jest w wyłącznym posiadaniu adresata informacji, tylko on może ją odczytać. Natomiast klucz publiczny jest udostępniony każdemu, kto zechce zaszyfrować wiadomość.

Historyjka graficzna, która wyjaśnia główna zasadę działania kryptografii z kluczem publicznym.



Krok 1: Alice przesyła do Boba swój klucz publiczny



Kroki 2 & 3: Bob szyfruje wiadomość kluczem publicznym Alice, która to następnie otrzymuje zaszyfrowaną wiadomość i rozszyfrowuje ją kluczem prywatnym.

Najpopularniejsze algorytmy kryptografii asymetrycznej:

- RSA
- ElGamal

Myślę, że to co jest powyżej wystarczy, jednak ambitniejsi mogą się zagłębić w zasady działania podpisu cyfrowego i w algorytm RSA, link poniżej:

Źródło: http://pl.wikipedia.org/wiki/Kryptografia_asymetryczna