**Wykład 4 (22.03.2022)**

Próbowala faktoryzowac klucz RSA… Teraz szuka jej cała Polska?

Szyfry asymetryczne

- para kluczy – jawny i tajny – nie ma problemu z dystrybucja klucza kryptograficznego

- metoda symetryczna – szybkość !!!

Dwa komplementarne klucze – prywatny , publiczny

Nie sa to losowe wygenerowane ciągi binarne

Niemozliwy losowy klucz – dwa klucze sa w pewien sposób zależne od siebie

Zachowanie poufności jest możliwe

Jeden z kluczy zachowujemy tylko dla siebie, drugi (publicny) powinien być znany wszystkim z którymi chcemy wymieniac dane,

Jeżeli przetworzymy tekst jawny za pomocą jednego to odszyfrowujemy tylko za pomocą tego drugiego, nigdy nie używamy tego samego klucza do szyfrowania i odszyfrowywania,

Zachowanie poufności – bierzemy klucz publiczny odbiorcy – szyfrujemy dane za pomocą tego klucza – w ten sposób zaszyfrowane dane może odczytac tylko wlasciciel pewnego klucza tajnego,

Podpis cyfrowy – jesli chcemy potwierdzić ze to my – ten dokument szyfrujemy za pomocą własnego klucza prywatnego – ten szyfrogram doklejamy do dokumentu – inne osoby sa w stanie zweryfikować ze to my pobierając nasz klucz publiczny i deszyfrują ten doklejony szyfrogram – jeśli otrzymają po deszyfrowaniu oficjalny dokument to znaczy ze tylko my byliśmy w stanie podpisac ten dokument

Wielkie ilości danych szyfrujemy algorytmami symetrycznymi – klucz przesylany odiorcy w celu zdeszyfrowania szyfrujemy asymetrycznie – klucz kryptograficzny (symetryczne) nie jest przesylany jawnie – wydajna bezpieczna kryptografia!!!

Kazda dowolna liczbe zlozona można przedstawić za pomocą sumy poteg liczb pierwszych

PIERWIASTKI PIERWOTNE – NOWE COSIK – potrzebne

RSA (potegowanie i operacja modulo)

EIGamal ( logarytmy dyskretne i operacja modulo)

RSA – najstarsz alg. Asymetryczny, popularny w srodowisku sieciowym, prosty do zrozumienia

Na slajdziorach…

Musimy w odpowiedni sposób dobrac dane które chcemy przeslac do odbiorcy,

Jeśli chcemy przesylac sobie duze ilości danych musimy dzielic je bloki o odpowiedniej wielkości,

- problem z szybka faktoryzacja dużych liczb

EIGamal – slajdzory…

Slaboscia kryptografii asymetrycznej jest bezpieczeństwo warunkowe.

Podsumowanie

Pamietac o dwóch kluczach – jak działajo

Zapytać na labie dlaczego warunkowo bezpieczny.