Wykład .

Temat: Inne algorytmy z kluczem publicznym: Diffiego-Hellmana, ElGamala, podpisu cyfrowego, na podstawie krzywej eliptycznej.

Algorytm Diffiego-Hellmana.

W 1976 r. Whitfield Diffie i Martin Hellman zaproponowali swój algorytm z kluczem publicznym przeznaczony do rozwiązania problemu dystrybucji kluczy dla kryptosystemów symetrycznych. Cel polegała na tym, żeby wymyślić bezpieczny sposób wspólnego ustalania klucza tajnego bez potrzeby wysyłania klucza innym sposobem, lecz korzystając z tej samej metody komunikacji, którą należało chronić.

Algorytm Diffiego-Hellmana nie można stosować do szyfrowania i odszyfrowania informacji!

Algorytm Diffiego-Hellmana działa następująco:

1. Niech mamy dwie osoby A i B, które chcą porozumieć się bezpiecznie, a więc potrzebują klucza szyfrowania.
2. Osoby A i B ustalają dwie duże liczby całkowite a i b takie, ze $1 < a < b$.
3. Osoba A wybiera przypadkowa liczbę i, oblicza $I = a^i \bmod b$ oraz wysyła I do osoby B.
4. Osoba B wybiera przypadkowa liczbę j, oblicza $J = a^j \bmod b$ po czym wysyła J do osoby A.
5. Osoba A oblicza klucz $k1 = J^i \bmod b$.
6. Osoba B oblicza klucz $k2 = I^j \bmod b$.
7. Wtedy mamy $k1 = k2 = a^{ij} \bmod b$, a więc $k1$ i $k2$ są kluczami tajnymi do stosowania przy właściwej transmisji.

Jeżeli ktoś przysłuchuje się przekazowi w sieci, będzie znał a, b, I oraz J. Jednak i oraz j pozostaną tajne. Bezpieczeństwo systemu zależy od trudności znalezienia:

- i znając $I = a^i \bmod b$

oraz

- j znając $J = a^j \bmod b$.

Ten problem, który nazywa się dyskretnym problemem logarytmicznym, jest uznany za trudny (to znaczy jest niewykonywalny dla współczesnej mocy obliczeniowej komputerów) przy większych wartościach. Tak więc a i b muszą być starannie wybrane i powinny być liczbami pierwszymi o długości co najmniej 512 bitów.

Algorytm ElGamala.

Rozszerzona w 1985 r. wersja algorytmu Diffiego-Hellmana przez Tahera ElGamala umożliwiła szyfrowanie, jak i uwierzytelnianie. Algorytm ElGamala nie został opatentowany (w przeciwieństwie do RSA), a więc stanowi potencjalnie mniej kosztowną alternatywę. Ponieważ opiera się on na algorytmie Diffiego-Hellmana, bezpieczeństwo informacji zależy od trudności obliczenia logarytmów dyskretnych.

Algorytm podpisu cyfrowego.

Algorytm podpisu cyfrowego DSA (Digital Signature Algorithm) został zaproponowany przez rząd USA jako standardowy algorytm dla podpisów elektronicznych. Opiera się on na algorytmie ElGamala, ale umożliwia tylko uwierzytelnianie. Nie dostarcza utajnienia.

Algorytm na podstawie krzywej eliptycznej.

Sposób szyfrowania i autoryzacji informacji na podstawie krzywej eliptycznej ECC (Ellittic Curve Cryptography) stosowany (od 1985 r.) do utajniania przekazów transmitowanych głownie przez sieć bezprzewodowa. Uważa się, ze te kryptosystemy opierają się na innych zasadach matematycznych niż podzielniki lub dyskretny problem logarytmiczny. Algorytm ECC, w porównaniu z algorytmem RSA czy Diffiego-Hellmana, stanowi bardziej wydajną technikę szyfrowania informacji. Na przykład taką samą moc kryptograficzną przy kluczu 1024-bitowym dla RSA można osiągnąć w ECC za pomocą klucza o długości 163 bity lub mniej.