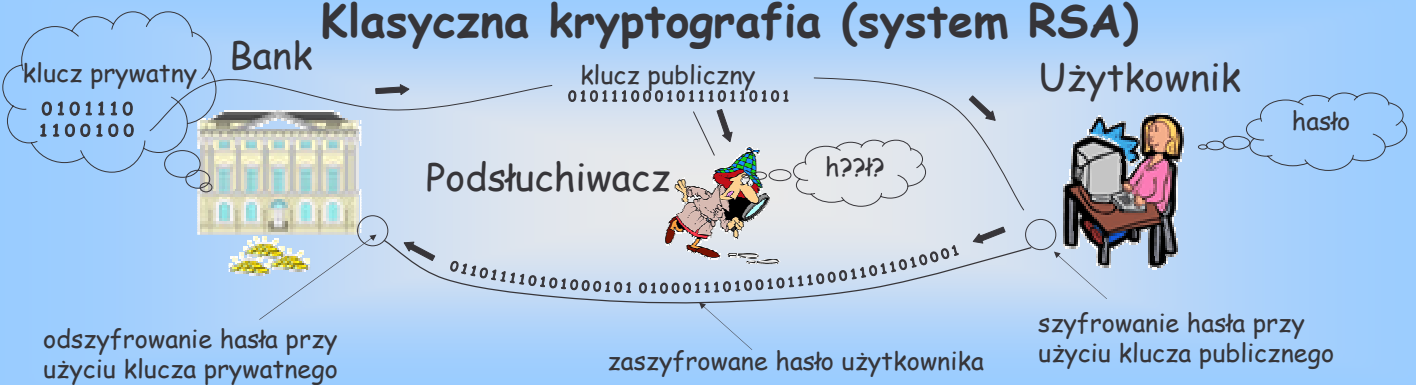


Kwantowe przelewy bankowe

Klasyczna kryptografia (system RSA)



Szyfrowanie w Internecie

- Konieczne wszędzie tam gdzie przesyłamy tajną informację:
 - przelewy bankowe, transakcje internetowe
 - logowanie przy użyciu SSH
- Używany system szyfrowania: RSA
 - szyfr z kluczem publicznym
 - bank wysła do użytkownika, bez szyfrowania, pewną liczbę, która pozwala zaszyfrować informację, ale jej znajomość nie wystarcza do łatwego rozszyfrowania.

Problemy z RSA

- Bezpieczeństwo: wiara w trudność wykonania rozkładu liczby na czynniki pierwsze
- Szybki algorytm rozkładu na czynniki pierwsze złamie system RSA
 - Taki algorytm już istnieje!
 - Algorytm Shora. Ale do działania potrzebuje komputera kwantowego. Więc póki co RSA można używać.

Kwantowa kryptografia (system BB84)



Działanie BB84

Bezpieczeństwo: gwarantowane prawami fizyki kwantowej.

1. Bank wysła losowo jeden z czterech fotonów, mających umownie przypisane wartości logiczne: $|0^\circ\rangle = 0$, $|90^\circ\rangle = 1$, $|45^\circ\rangle = 0$, $|135^\circ\rangle = 1$
2. Użytkownik ustawia polaryzator przypadkowo w jednej z dwóch pozycji i sprawdza czy foton przeszedł, czy nie. Na tej podstawie ustala wartość bitu. (Jak przeszedł to 1, jak nie przeszedł to 0)

3. Przez telefon ogłaszają bazy jakich używali (tylko bazy nie wartości bitów). W tych przypadkach gdy bazy są zgodne zachowują bity jeśli nie to odrzucają.
 - Ujawniają część z pozostawionych bitów. Jeśli się zgadzają znaczy, że nikt nie podłuchiwał! - nie da się mierzyć polaryzacji nieznanego fotonu nie zaburzając go!
 - Mając sekretny klucz, mogą przestać tajną informację, o takiej co najmniej długości jakiej jest klucz.

Nie da się bez zaburzania rozróżnić fotonów o nie prostopadłych polaryzacjach: np. $|0^\circ\rangle$ i $|45^\circ\rangle$

Centrum Fizyki Teoretycznej PAN

X Piknik Naukowy, 3 czerwca 2006 r.