Opole, dn. 15 listopada 2005

Politechnika Opolska
Wydział Elektrotechniki i Automatyki
Kierunek: **Informatyka**

Seminarium Ochrony Danych

Temat:

Nowoczesne metody kryptograficzne

Autor: **Nitner Piotr**
Dawid Najgiebauer
Informatyka, rok 2005/06, sem. V,
grupa sem. 7 (Czw. g. 7.30)

Prowadzący: **mgr inż. Wiesław Kopterski**

Ocena: .....

Uwagi: .....

O P O L E 2 0 0 5

1.1. Spis treści

1.2. Spis rysunków

1. Kryptografia symetryczna i asymetryczna

Czym jest właściwie kryptografia? Słowo „kryptografia" pochodzi od greckich *kryptós* – „ukryty" oraz *gráphein* – „pisać". Czyli jest to nauka zajmująca się układaniem szyfrów. Wyróżniane są dwa główne nurty kryptografii:

- **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. Bezpieczeństwo takiego szyfrowania zależy od:
  - ilości możliwych kluczy, czyli długości klucza
  - odporności na ataki inne niż *brutal force*
- **Kryptografia asymetryczna** – to rodzaj kryptografii, w którym używa się co najmniej dwu powiązanych ze sobą kluczy, z których każdy używany jest na innym etapie kryptograficznym. 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, w niektórych innych zastosowaniach kluczy może być więcej.

Wszystkie tradycyjne szyfry miały charakter symetryczny. Jednak takie rozwiązanie zawierało wiele wad:

- Umożliwiały jedynie szyfrowanie wiadomości (brak możliwości wykorzystania do uwierzytelniania, podpisów cyfrowych lub innych zaawansowanych funkcji kryptograficznych).
- Niebezpieczeństwo przejęcia klucza przez „wroga", który za jego pomocą może zarówno podszywać się pod daną osobę rozsyłając zaszyfrowane wiadomości, jak i odczytywać takie wiadomości adresowane do tej osoby. Tak, więc klucz musi być utrzymywany w tajemnicy po obu stronach kanału komunikacji.
- Potrzeba stosowania ogromnej liczby kluczy np. w dużych sieciach w przypadku wielu komunikujących się osób.

Jednak w pewnych sytuacjach szyfrowanie symetryczne wciąż jest lepszym rozwiązaniem ze względu na:

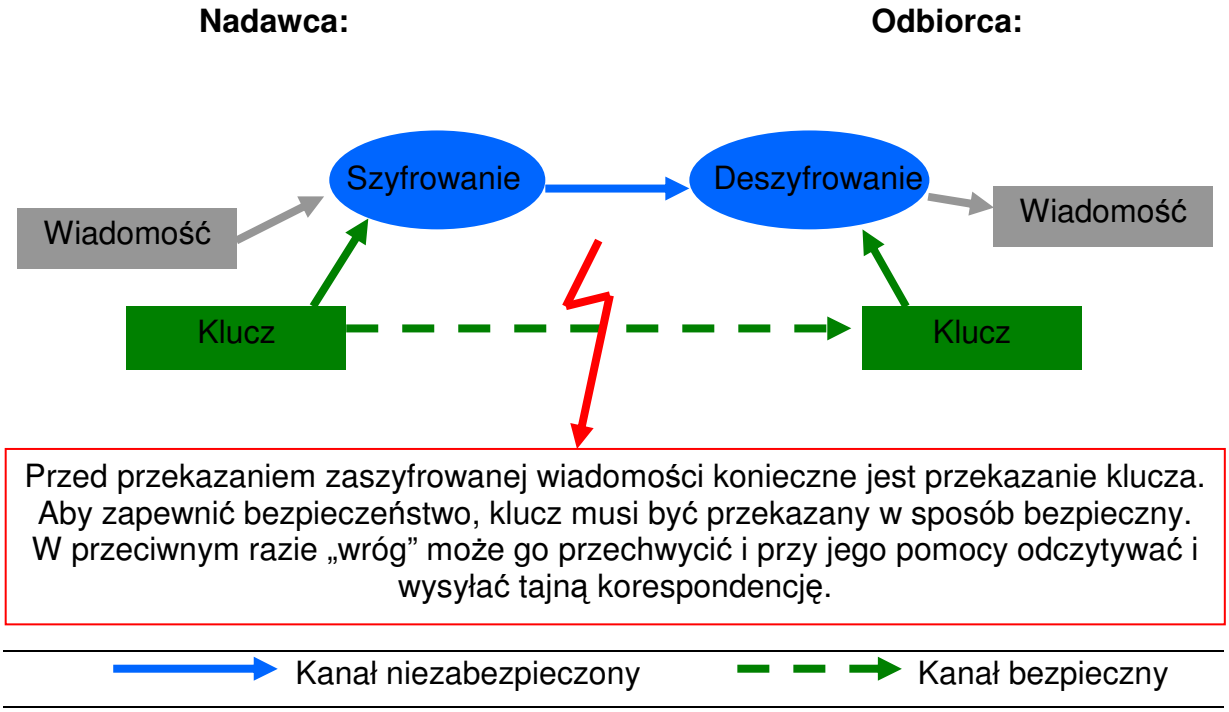
- Szybkość działania
- Relatywnie małą długość klucza

Oba rozwiązania charakteryzują się pewnymi wspólnymi cechami. Najczęściej są to operacje na poszczególnych bitach, jako najszybsze w realizacji. Stąd, mówiąc o sile danego algorytmu podaje się jego długość właśnie wyrażoną w bitach.

Zarówno klucz, jak i wygenerowana na jego podstawie zakodowana wiadomość mają charakter losowy. Dlatego do czasu, gdy nie znamy klucza deszyfrującego, niemożliwe jest odczytanie pierwotnej wiadomości.

Jeśli klucz użyty do szyfrowania jest na tyle długi, aby przy jego pomocy zakodować całą wiadomość wykorzystując go tylko jeden raz, to uzyskany kryptograf gwarantuje zdecydowanie większy poziom bezpieczeństwa. Jest to związane z faktem, że wielokrotne wykorzystanie klucza może prowadzić do wykrycia pewnych prawidłowości, na podstawie których złamanie szyfru może być zdecydowanie łatwiejsze.

2. Szyfrowanie symetryczne



Rysunek 2.1. *Schemat przekazywania wiadomości przy użyciu szyfrowania symetrycznego.*

Wśród kodowania symetrycznego najczęściej stosowanymi algorytmami są:

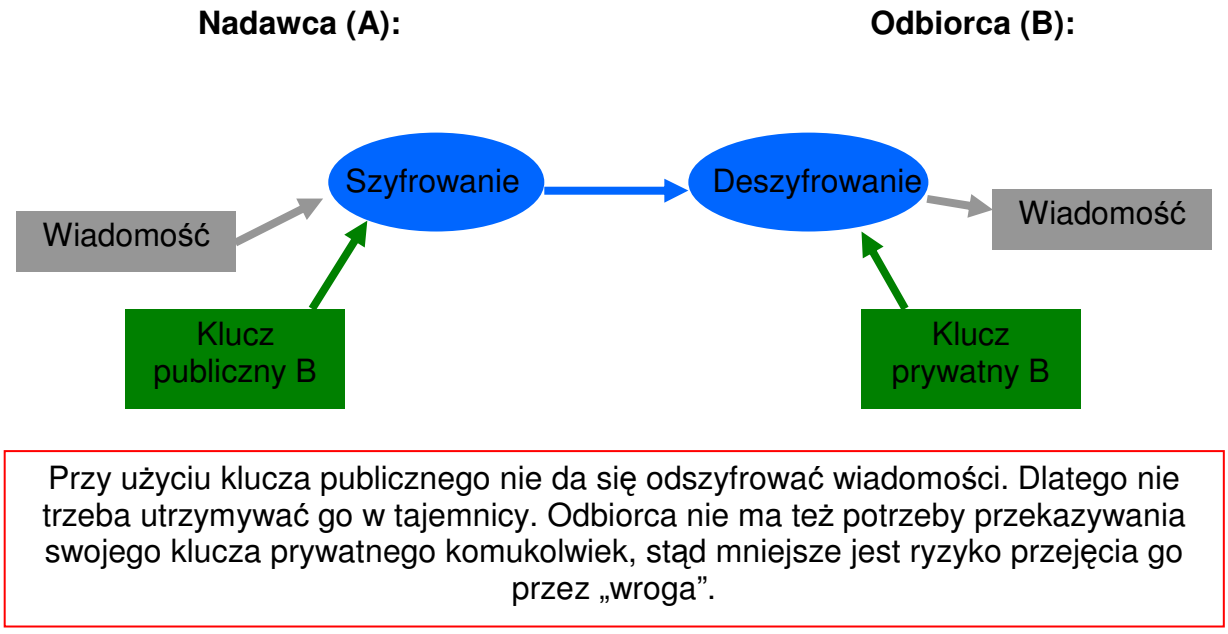
- **DES** (*Digital Encription Standard*) - został opracowany jeszcze w latach pięćdziesiątych przez pracowników firmy IBM. DES jest algorytmem blokowym wykorzystującym klucz 56-bitowy, zaakceptowanym przez rząd Stanów Zjednoczonych w 1977 jako standard szyfrowania danych bez klauzuli tajności. Z powodu słabości klucza został w dużej mierze zastąpiony przez inne szyfry: modyfikacje DESa takie jak 3DES czy DESX, a ostatnio przez nowsze i bezpieczniejsze algorytmy jak AES, IDEA, Twofish itd.
- **3DES** – algorytm polegający na zakodowaniu danej algorytmem DES przy użyciu pierwszego klucza, następnie zdekodowaniu przy użyciu drugiego klucza i ponownym zakodowaniu przy użyciu trzeciego klucza.
- **DESX** to prosta modyfikacja DESa: 1) blok danych XORujemy z pierwszym kluczem (64 bitowym); 2) blok szyfrujemy za pomocą DESa drugim kluczem (56 bitowym); 3) blok danych XORujemy z trzecim kluczem (64 bitowym).
- **IDEA** (*International Data Encryption Algorithm*) – algorytm blokowy z kluczem 128-bit operujący na 64-bitowych blokach danych opracowany pod koniec lat ‘80. IDEA była używana w początkowych wersjach PGP. Jednak ze względów patentowych oraz ze względu na powstanie lepszych algorytmów (AES) i postępy w kryptoanalizie IDEA znacznie straciła na popularności, choć nie została nigdy złamana.
- **Blowfish** – szyfr blokowy stworzony przez Bruce'a Schneier'a w 1993 roku jako szybka i bezpłatna alternatywa dla istniejących ówcześnie algorytmów.
- **Twofish** – stworzony przez tą samą osobę, co Blowfish. Operuje na 128-bitowych blokach przy użyciu kluczy o długości 128-, 192-, lub 256-bitów.
- **AES (Rijndael)** (*Advanced Encryption Standard*) – 128, 192 lub 256-bitowy algorytm operujący na 128-bitowych blokach danych (oryginalna specyfikacja Rijndael dopuszczała również bloki 192 i 256 bitowe). Został on stworzony w 1997 r. ze względu na niewystarczającą siłę algorytmu DES.
- **Serpent** – używający 128, 192 lub 256-bitowego klucza operujący na 128-bitowych blokach. Prawdopodobnie jest bezpieczniejszy od algorytmu AES, lecz jest od niego wolniejszy.

3. Szyfrowanie asymetryczne

Kryptografia asymetryczna została odkryta przez Martina Hellmana, Whitfielda Diffie i niezależnie przez Ralpha Merkle w 1976 roku. Dopiero pod koniec XX wieku brytyjska służba wywiadu elektronicznego ujawniła, że jej pracownik Jamesa Ellisa już w 1965 roku stworzył koncepcję kryptografii asymetrycznej, a działający system został stworzony w 1973 roku przez Clifford Cocks. Odkrycia te były jednak objęte klauzulą tajności do 1997 roku. Obecnie kryptografia asymetryczna jest szeroko stosowana tam, gdzie nie można zagwarantować poufności wymiany informacji (np. Internet). Stosowana jest także w systemach elektronicznego uwierzytelniania, obsługi podpisów cyfrowych i w wielu innych specyficznych zastosowaniach.

Algorytmy mające zastosowanie w kryptografii asymetrycznej wykorzystują operacje, które da się łatwo przeprowadzić w jedną stronę a bardzo trudno w drugą. Np. mnożenie jest łatwe, a faktoryzacja (znalezienie dwóch liczb, które po pomnożeniu dadzą określony wynik) trudna (na czym opiera się RSA). Podobnie: potęgowanie modulo jest łatwe, a logarytm dyskretny jest trudny (na czym opierają się ElGamal, DSA i ECC).

W procesie przekazywania tajnej wiadomości, klucz publiczny używany jest do jej zaszyfrowania, a klucz prywatny do jej odczytu. Ponieważ klucz prywatny jest w wyłącznym posiadaniu adresata informacji i nie powinien być on nikomu udostępniany, tylko on może odczytać informację. Natomiast klucz publiczny jest udostępniony każdemu, kto zechce przesłać do danej osoby zaszyfrowaną wiadomość.



Rysunek 3.1. *Schemat przekazywania wiadomości przy użyciu szyfrowania asymetrycznego.*

Ponieważ kryptografia asymetryczna jest o wiele wolniejsza od symetrycznej, prawie nigdy nie szyfruje się całych wiadomości przy jej wykorzystaniu. Zamiast tego szyfruje się jedynie klucz szyfru symetrycznego, którym to dopiero szyfrowana jest właściwa wiadomość.

Wśród algorytmów asymetrycznych wyróżnia się:

- **RSA** (*od nazwisk twórców*) – to pierwszy i obecnie jeden z dwóch najpopularniejszych algorytmów kryptografii asymetrycznej. Stworzony w roku 1978 przez zespół: Ronald Rivest, Adi Shamir, Leonard Adleman. RSA opiera się na trudności faktoryzacji dużych liczb – znalezienie szybkiej metody faktoryzacji (znalezienia dwóch takich liczb, których pomnożenie przez siebie da w wyniku liczbę) doprowadziłoby do złamania RSA, aczkolwiek nie ma dowodu, że nie da się złamać RSA w inny sposób. Jak dotąd (maj 2004) udały się ataki na klucze o długości do ok. 600 bitów.
- **ElGamal** – Trudność złamania tego system jest oparta na problemie liczenia logarytmu dyskretnego.

3.1. Algorytm RSA

Żeby wyznaczyć klucz RSA losujemy dwie duże liczby pierwsze p i q oraz liczbę względnie pierwszą[1] e z $(p-1)(q-1)$. Następnie obliczamy $d=e^{-1} \bmod (p-1)(q-1)$ oraz $n=p*q$. Klucz publiczny to para (e,n), klucz prywatny zaś to para (d,n). Liczby p i q należy zniszczyć.

Żeby szyfrować podnosimy liczbę reprezentującą wiadomość do potęgi e modulo n:

$c = m^e \bmod n$

Żeby ją zdeszyfrować podnosimy zaszyfrowaną wiadomość do potęgi d:

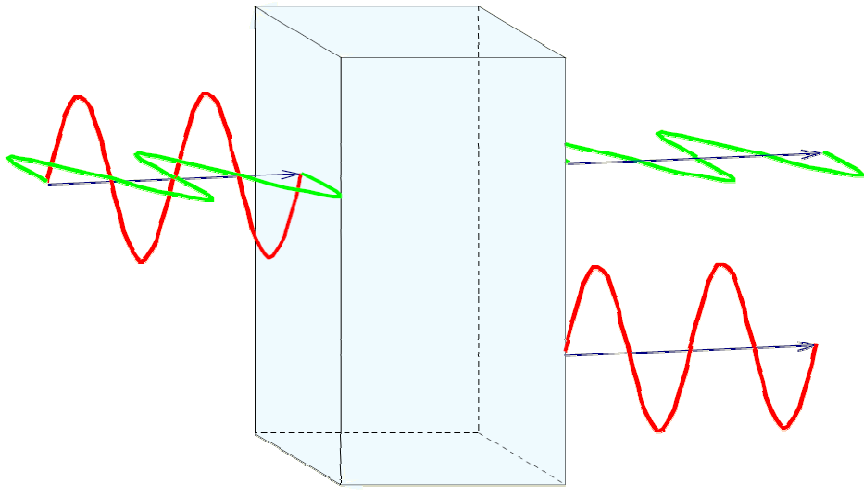
$m = c^d \bmod n$

[1] Liczby, których największym wspólnym dzielnikiem jest liczba 1.

4. Kryptografia kwantowa

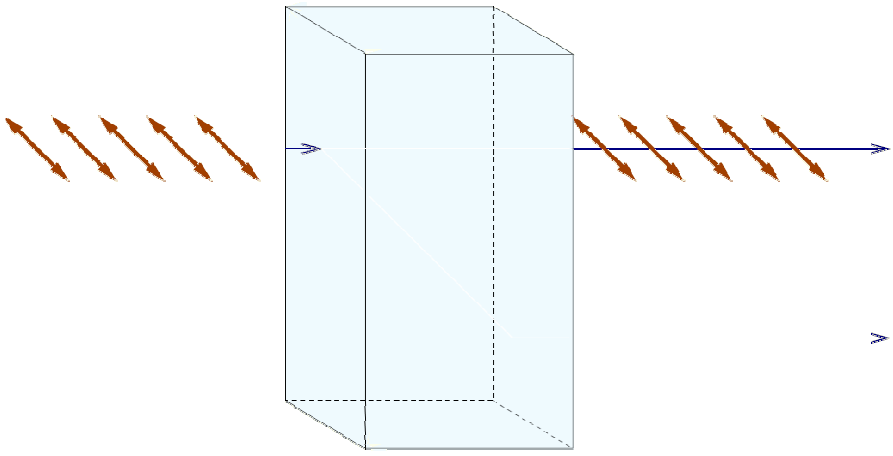
W technice kwantowej wykorzystuje się światło do przenoszenia informacji. Światło, jak wiadomo, jest falą składającą z fal drgających w różnych kierunkach. Możliwe jest jednak spolaryzowanie fali, co spowoduje jej drganie wyłącznie w jednym kierunku.

Ciekawymi właściwościami względem fal spolaryzowanych wykazuje się np. dwójłomny kryształ kalcytu. Rozdziela falę świetlną na dwie składowe o wzajemnie prostopadłych polaryzacjach (promień zwyczajny i nadzwyczajny).

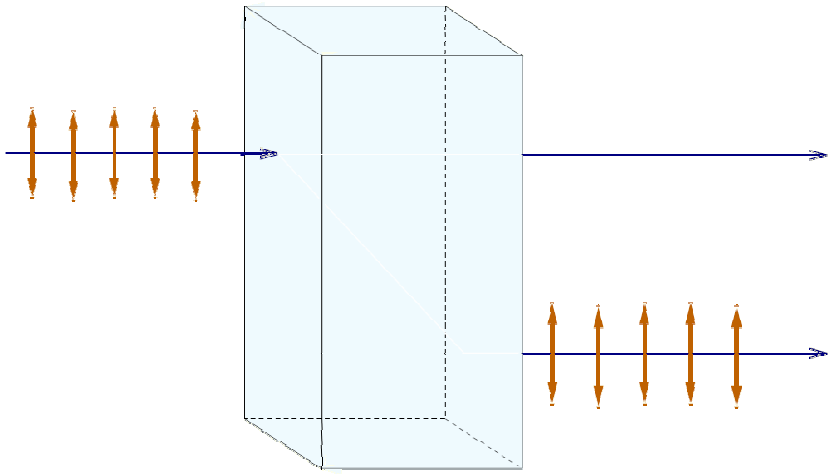


Rysunek 4.1. *Rozdzielanie fali świetlnej przez dwójłomny kryształ kalcytu.*

Poziomo spolaryzowane fotony padające na kryształ przechodzą przez niego bez zmiany kierunku propagacji tworząc promień zwyczajny (rys. 4.2), zaś spolaryzowane pionowo zostają odchylone tworząc promień nadzwyczajny (rys. 4.3).

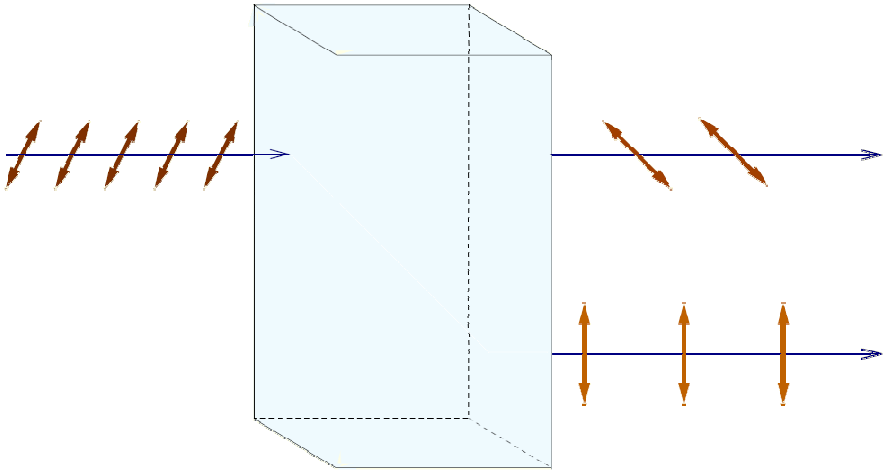


Rysunek 4.2. *Zachowanie się fotonów spolaryzowanych poziomo przy przechodzeniu przez kryształ.*



Rysunek 4.3. *Zachowanie się pionowo spolaryzowanych fotonów przy przechodzeniu przez kryształ.*

W przypadku, gdy mamy do czynienia z polaryzacją ukośną, fotony padające na kryształ otrzymują polaryzację pionową lub poziomą z prawdopodobieństwem 50% dla każdej z nich. Po przejściu przez ten kryształ nie niosą już jednak one z sobą żadnych informacji o pierwotnej polaryzacji.



Rysunek 4.4. *Zachowanie się ukośnie spolaryzowanych fotonów.*

Pomiar polaryzacji fotonów po przejściu przez kryształ fotonów spolaryzowanych doń ukośnie nie da żadnej informacji o początkowej polaryzacji. Można tą polaryzację odczytań poprzez odwrócenie kryształu o 45° (odczyt tzw. bazy ukośnej). Wtedy jednak nie będzie możliwy odczyt polaryzacji 0° i 90° (tzw. bazy prostej).

Fakt, że wyniki pomiarów w mechanice kwantowej mają charakter losowy umożliwia, bezpieczne przekazywanie klucza kryptograficznego!

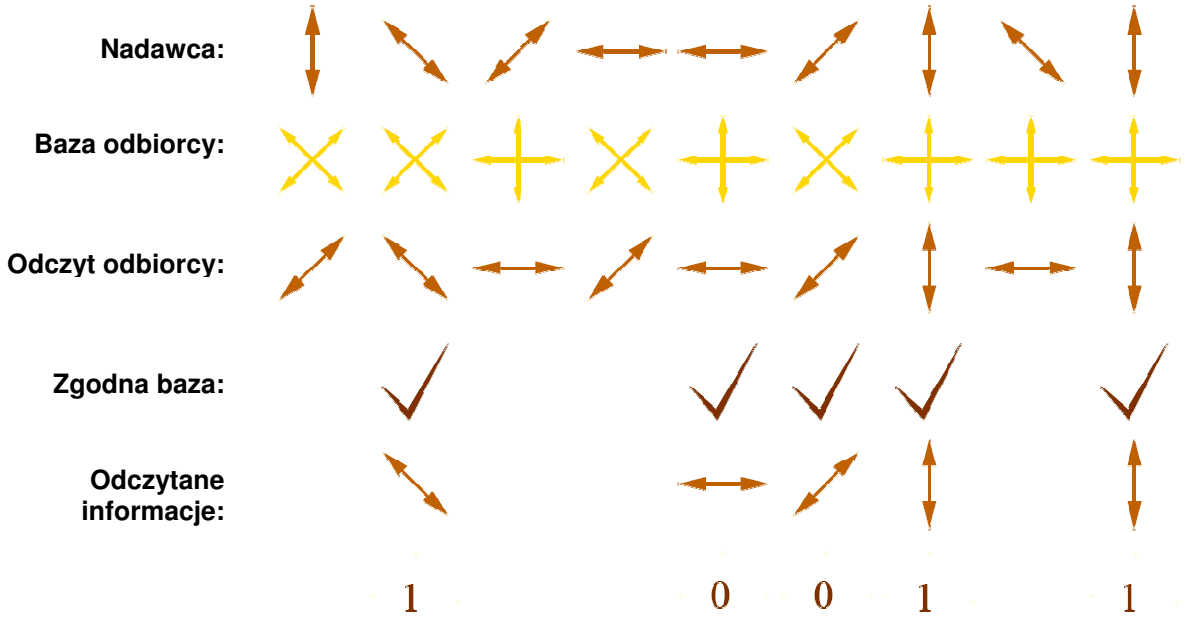
Polaryzacja prosta i polaryzacja ukośna to dwie wielkości fizyczne, które zgodnie z prawami mechaniki kwantowej nie są współmierzalne. Pomiar jednej z nich czyni drugą całkowicie nieokreśloną. Mamy tu do czynienia z zasada nieoznaczoności Heisenberga. Fakt ten może w prosty sposób zostać wykorzystany do stwierdzenia, że transmisja jest podsłuchiwana przez „wroga”.

Na podstawie powyższych właściwości możemy określić dwa „alfabety” kwantowe – prosty i ukośny.

Rysunek 4.5. *Alfabet kwantowy prosty i ukośny.*

Schemat przesyłu danych:

1. Nadawca wybiera losowo jedną z czterech polaryzacji i wysyła do odbiorcy foton o takiej polaryzacji. Ciąg fotonów o określonych polaryzacjach stanowi ciąg zer i jedynek z dwóch alfabetów kwantowych.
2. Odbiorca wybiera losowo bazę prostą lub ukośną i wykonuje pomiar polaryzacji fotonu, który otrzymał od nadawcy.
3. Odbiorca notuje wyniki pomiarów zachowując je w tajemnicy.
4. Odbiorca publicznie informuje nadawcę, jakiej bazy używał do pomiaru, zaś nadawca publicznie informuje go czy wybrana przez niego baza była właściwą czy nie.
5. Nadawca i odbiorca przechowują wyniki pomiarów, dla których odbiorca użył właściwej bazy. Uzyskany w ten sposób losowy ciąg zer i jedynek może stanowić klucz kryptograficzny.



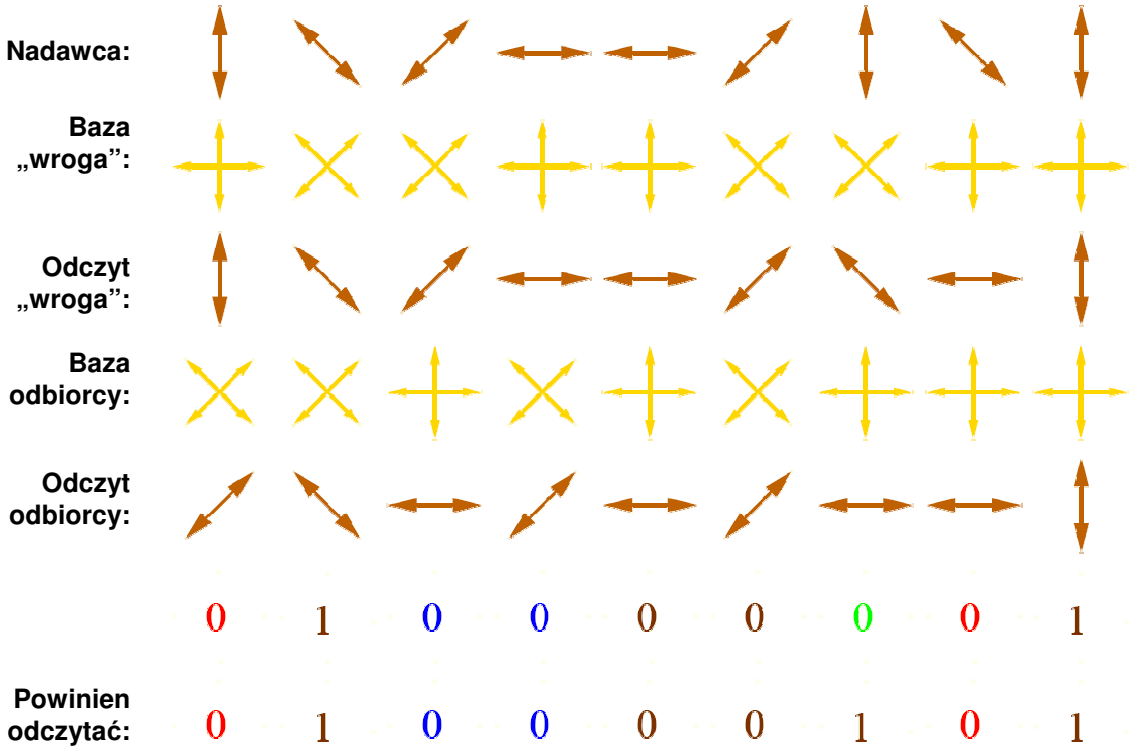
Rysunek 4.6. *Ustalanie klucza przy użyciu metod kryptografii kwantowej.*

Średnio 50% bitów zarejestrowanych przez odbiorcę to bity pewne (pozostawione), 25% bitów to bity prawidłowe mimo złego wyboru bazy i 25% to bity nieprawidłowe.

W przypadku podsłuchiwania, transmisja przebiega następująco:

1. „Wróg" podsłuchuje dokonując pomiaru w losowo wybranej bazie.
2. Po zarejestrowaniu polaryzacji przesyła foton o takiej samej polaryzacji do odbiorcy. W ten sposób „wróg" zmienia niektóre bity, czyli prowadza błędy w przekazie (bity zielone).
3. Nadawca i odbiorca mogą wykryć obecność „wroga" porównując losowo wybraną część bitów z uzgodnionego juz klucza (bity te następnie usuwają).

4. Jeśli okaże się, że bity zostały zmienione, to oznacza ze „wróg” podsłuchiwał. Wtedy uzgadnianie klucza rozpoczyna się od nowa.



Rysunek 4.7. *Podsłuchiwanie transmisji kwantowej.*

Niezaprzeczalną zaletą w poufności transmisji kwantowej jest fakt, iż nie ma możliwości pasywnego podsłuchu. Każdy podsłuch zaburza przekaz. W ten sposób prawa mechaniki kwantowej gwarantują bezpieczeństwo przy uzgadnianiu klucza kryptograficznego. Kwantowa dystrybucja klucza w połączeniu z mocnym algorytmem szyfrującym tworzą bezpieczny kanał łączności.

Obecnie wciąż pojawiają się nowe metody wykorzystania techniki kwantowej w dziedzinie kryptografii. Choć już na dzień dzisiejszy jest to produkt wykorzystywany komercyjnie. Istnieje kilka firm, które produkują urządzenia do kryptografii kwantowej, m.in. NEC i Toshiba. Uruchomiono też pierwsze sieci z kwantową dystrybucją klucza, a eksperymentalnie dokonano pierwszych przekazów wideo szyfrowanych kluczem kwantowym. Unia Europejska zainwestuje 11 mln € w ciągu 4 lat w system SECOQC (Secure Communication based on Quantum Cryptography).

5. Bibliografia

1. http://pl.wikipedia.org/wiki
2. http://www.rsasecurity.com/rsalabs/faq/index.html
3. http://csrc.nist.gov/encryption/aes/aesfact.html
4. http://www.chip.pl/arts/archiwum/n/articlear_69826.html
5. http://krystian.jedrzejczak.webpark.pl/bezp2.htm
6. http://www.bezpieczenstwoit.pl/Artykuly/Kryptografia/T.Adamski_Algorytm_RSA-podstawy_teoretyczne/
7. http://zon8.physd.amu.edu.pl/~tanas