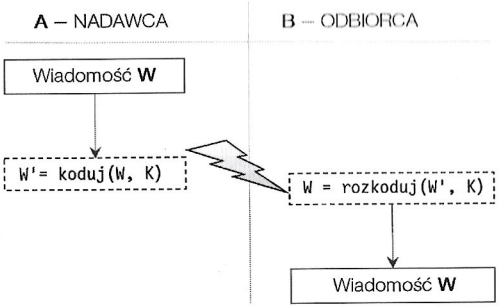
Wynik działania (na konsoli możesz zobaczyć spacje zamiast niektórych symboli):

```
Klasyczna metoda XOR
Oryginał:  Ala ma kota
Ciąg zakodowany XOR:  bOB NB
Metoda 255
Oryginał:  Figo to pies
Ciąg zakodowany XOR:  ¹  ß  ß
Ciąg odkodowany XOR:  Figo to pies
```

Kodowanie symetryczne

Kodowanie pasjonowało ludzi od wieków i czyniono wielkie starania, aby wymyślać takie algorytmy kodujące, które byłyby trudne do złamania w rozsądnym czasie. Pierwsze metody kodowania realizujące te wymagania, które zostały rozpowszechnione, zwane są *symetrycznymi*. Proces kodowania i dekodowania w kodowaniu symetrycznym można przedstawić w postaci prostego schematu zaprezentowanego na rysunku 18.1.



RYSUNEK 18.1. Kodowanie symetryczne

Wiadomość `W` jest szyfrowana przez nadawcę `A` za pomocą procedury szyfrującej `koduj`, która przyjmuje dwa parametry, czyli tekst do zaszyfrowania i pewien dodatkowy parametr `K`, zwany kluczem. Klucz `K` pełni funkcję elementu komplikującego powszechnie znany algorytm kodowania (np. tabelkę odwzorowującą znaki na liczby) i ma na celu utrudnienie odczytania wiadomości osobom niepowołanym.

Odbiorca `B` otrzymuje zaszyfrowaną (nieczytelną) wiadomość `W'`, ale mając do dyspozycji procedurę odkodowującą i dysponując kluczem `K`, bez trudu poradzi sobie z odtworzeniem wiadomości `W`. Po stronie odbiorczej klucz `K` jest używany do rozkodowania lub do wyliczenia finalnego klucza rozkodowującego i odczytania informacji.

Aby zapewnić poufność, przed rozpoczęciem wymiany informacji nadawca i odbiorca muszą wymienić się kluczem. W realizacjach fizycznych metod kodowania symetrycznego klucz jest automatycznie generowany i wymieniany (w postaci zaszyfrowanej!) z odbiorcą przed rozpoczęciem transmisji.

Przykład szyfrowania z użyciem kodu symetrycznego:

- Przypisujemy literze alfabetu wartość liczbową — jest to zwykłe kodowanie tabelkowe, bardzo zresztą łatwe do złamania przez językoznawców uzbrojonych w komputerowe „liczydło" i swoją wiedzę.
- Jak skomplikować ten powszechnie znany algorytm kodowania? Można np. dodać do przesyłanej liczby kodowej pewną wartość K, co spowoduje, że niemożliwe stanie się odczytanie wiadomości za pomocą zwykłego porównywania pozycji tabelki kodującej.
- Odbiorca B, zanim rozpocznie dekodowanie, powinien odjąć od otrzymanych liczb liczbę K, tak aby otrzymać kanoniczny kod tabelkowy[3].

Łatwo dostrzec zasadniczą niedogodność takiego systemu kodującego, przyglądając się rysunkowi 18.1: nadawca i odbiorca muszą znać wartość klucza K. Przesyłanie konwencjonalnymi metodami klucza, np. przez kuriera, jest bardzo niepraktyczne i na dodatek naraża na niebezpieczeństwo zarówno poufność danych jak i... samego kuriera! Ponadto klucz jest dość prymitywny i mając wystarczająco dużo czasu, można się pokusić o próbę odtworzenia wiadomości, stosując kolejne wartości klucza. Nietrudno zatem dojść do wniosku, że *kodowanie symetryczne* jest słabą metodą, do jej złamania wystarczy bowiem kradzież klucza, próby jego odgadnięcia lub metody inżynierii odwrotnej (ang. *reverse engineering*).

Mimo to algorytmy symetryczne mają dużą zaletę: są szybkie! Niektóre ciekawe algorytmy szyfrujące symetrycznie zostały opublikowane i stały się częścią protokołów i znanych programów. Przykładem może być algorytm DES (ang. *Data Encryption Standard*), czyli szyfr blokowy, w którym dane są szyfrowane blokami o długości 64 bitów (tj. 8 znaków ASCII wyposażonych w bit parzystości).

W DES klucz ma długość 56 bitów, choć jest zapisywany za pomocą 64 bitów (co ósmy bit jest bitem parzystości). W ciele algorytmu wykonywane są cykliczne permutacje i mieszania bloków danych. Modyfikacja oryginalnego ciągu zależy od wartości podkluczy K_1, K_2, ..., K_{16} wygenerowanych na podstawie klucza podanego przez użytkownika (K_0). Podklucze są używane do permutacji i mieszania bloków danych w kolejnych turach przetwarzania algorytmu. Proces odkodowania korzysta z tych samych podkluczy, ale w odwrotnej kolejności.

Algorytm DES jest stosowany do kodowania załączników w poczcie elektronicznej. Niegdyś był szeroko wykorzystywany w przemyśle, np. w branży finansowej, obecnie w jego miejsce stosuje się raczej jego silniejszą odmianę o nazwie 3DES z kluczem 168 bitów, trudniejszą do złamania.

W DES dla każdej wiadomości klucz wybierany jest losowo spośród 72 000 000 000 000 000 (72 kwadrylionów) możliwych; wiadomości szyfrowane za pomocą algorytmu DES uważane były za niemożliwe do złamania. W 1997 r. firma RSA

(będąca właścicielem opisywanej dalej w tym rozdziale innej metody kryptograficznej) ustanowiła nagrodę w wysokości 10 000 dolarów za sforsowanie algorytmu DES. Wysiłki powołanej do tego celu grupy i wolne moce kilkunastu tysięcy komputerów użytkowników Internetu zaowocowały złamaniem kodu w niecałe trzy miesiące. Dziesięć lat później Frontier Foundation polepszyła ten wynik, łamiąc zakodowany w DES tekst w dziewięć dni; wkrótce pojawiły się też oferty sprzętowych kodołamaczy (np. projekt COPACOBANA), czyli specjalizowanych komputerów zoptymalizowanych w celu łamania kodów za pomocą różnych metod (głównie rozmaitych metod siłowych).

Warto wiedzieć, że istnieją kodery sprzętowe (oparte na układach scalonych) DES, które są średnio 1000 razy szybsze od wersji software'owych.

Kodowanie asymetryczne

Kodowanie asymetryczne eliminuje wadę związaną z kłopotliwą logistyką i pilnowaniem kluczy napotkaną w algorytmach symetrycznych. Rozwiązuje efektywnie *problem transmisji klucza* w świecie, gdzie ważne jest, aby wiadomość dotarła do odbiorcy w ułamku sekundy, bez obarczania go dodatkową troską o wiarygodność otrzymanego klucza K.

Zakłada się, że odbiorca pragnący otrzymać wiadomość może wysłać nadawcy klucz szyfrujący w sposób jawny. Nadawca zaszyfrowuje nim swoją wiadomość i wysyła ją do odbiorcy przez publiczne łącza transmisyjne — podczas transmisji jest zatem zachowana poufność. Odbiorca odszyfrowuje ją *innym* kluczem, będącym wyłącznie w jego posiadaniu. Przechwycenie klucza szyfrującego, bez drugiego klucza — odszyfrowującego, nic nie daje!

Pierwszy klucz, szyfrujący, nazywa się *kluczem publicznym*, a drugi, odszyfrowujący — *kluczem prywatnym*. Klucza prywatnego należy strzec jak oka w głowie, a klucz publiczny można swobodnie rozdawać tym, z którymi chcemy się komunikować. Każdy, kto otrzymał klucz publiczny, będzie mógł wysłać do nas zaszyfrowaną nim wiadomość, którą odczytamy tylko my, jako jedyni posiadacze klucza prywatnego.

Metodę kodowania z kluczem publicznym, która całkowicie wyeliminowała dystrybucję klucza, wynaleziono w 1976 r. Jej wynalazcami byli Whitfield Diffie i Martin Hellman, jednak jej pierwsza praktyczna realizacja została opracowana przez Rona Rivesta, Adiego Shamira i Leonarda Adlemana; jest znana jako tzw. kryptosystem *RSA*. Metoda RSA gwarantuje bardzo duży stopień bezpieczeństwa przesyłanej informacji. Ponieważ została uznana przez matematyków za niemożliwą do złamania, momentalnie stała się obiektem zainteresowania komputerowych maniaków na całym świecie, którzy za punkt honoru przyjęli jej złamanie[4].

---

[4] Prawa do algorytmu RSA posiada *RSA SECURITY LLC* (obecnie część EMC Corporation), udzielająca płatnej licencji na jego używanie w programach innych producentów (skorzystano z niej w takich produktach jak Internet Explorer i Netscape Navigator). RSA