

Kodowanie i kryptografia

Wprowadzenie

dr Robert Borowiec

Politechnika Wrocławska

Instytut Telekomunikacji i Akustyki

pokój 908, C-5

tel. 3203083

e-mail: robert.borowiec@pwr.wroc.pl

www: lstwww.ita.pwr.wroc.pl/~RB/

Wykład I

1-godzina

Literatura z kodowania

1. W. Mochnecki, *Kody korekcyjne i kryptografia*, Wyd. Politechniki Wrocławskiej, 1997.
2. Simon Haykin, *Systemy telekomunikacyjne*, WKŁ, Warszawa 1998 r.
3. D.J.Bem, *Kodowanie - materiały do wykładu*, dostępne w punkcie ksero.

Literatura z kryptografii

1. W. Mochnaeki, *Kody korekcyjne i kryptografia*, Wyd. Politechniki Wrocławskiej, 1997.
2. D. E. R. Denning, *Kryptografia i ochrona danych*, WNT, Warszawa, 1993.
3. B. Schneier, *Kryptografia dla praktyków*, WNT, Warszawa, 1995.
4. N. Koblitz, *Wykład z teorii liczb i kryptografii*, WNT, Warszawa, 1995.
5. M. R. Ogiela, *Podstawy Kryptografii*, Wydawnictwa AGH, Kraków 2000 r.

Robert Borowiec

Kryptografia, Wykład I,
Systemy cyfrowe, strona 3/13

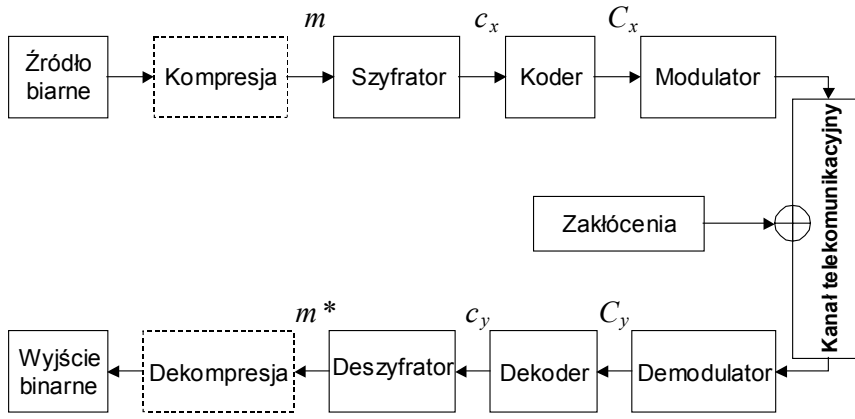
Literatura z modulacji cyfrowych

1. Tri T. Ha, *Digital satellite communications*, Macmillan Publication Company, New York, Collier Macmillan Publishers, London 1986.
2. S. Benedetto, E. Biglieri, V. Castelloni, *Digital transmission theory*, Prentice-Hall, Englewood Cliffs, New Jersey, 1987
3. R. Steele, *Mobile radio communications*, Pertech Press Publishers, London, 1992.
4. S. Haykin, *Systemy telekomunikacyjne*, (cz. 1 i 2), WKiŁ Warszawa, 1998

Robert Borowiec

Kryptografia, Wykład I,
Systemy cyfrowe, strona 4/13

Cyfrowy system transmisyjny



Robert Borowiec

Kryptografia, Wykład I,
Systemy cyfrowe, strona 5/13

Pojęcia podstawowe

Źródło binarne – dowolne urządzenie (np.: komputer, modem, przetwornik A/C) generujące równomiernie strumień bitów z prędkością R , zwaną *przepływnością binarną*:

$$R = \frac{1}{T} \left[\frac{\text{bit}}{s} \right]$$

Bity na wyjściu źródła pojawiają się w odstępach czasu T , tzw. *jednostkowego odstępu wymiany*

Robert Borowiec

Kryptografia, Wykład I,
Systemy cyfrowe, strona 6/13

Pojęcia podstawowe

Kompresja danych - stosowana jest po to, aby zmniejszyć ilość przesyłanych danych bez uszczerbku dla zawartej w nich informacji. Rozróżniamy dwa podstawowe sposoby kompresji:

- ☐ ilościowa (bezstratna)
- ☐ jakościowa

Kompresja ilościowa - wykorzystuje redundancję źródła informacji.

Kompresja jakościowa - wykorzystuje ułomność zmysłów człowieka (zgadzamy się na niezauważalną utratę ilości informacji).

Pojęcia podstawowe

Kodowanie kanałowe - stosowane jest po to, aby zapewnić przy określonym stosunku E_b/N_o (energii bitu do energii szumu) odpowiednią jakość transmisji. Kodowanie jest procesem wprowadzania informacji nadmiarowej, którą potem dekodery wykorzystują do oceny odebranych informacji.

Układ **koder-dekoder** ma, więc za zadanie zmniejszenie wpływu szumu na jakość transmisji. Wprowadzenie informacji nadmiarowej (bitów kontrolnych) implikuje wzrost prędkości strumienia bitów, a więc i szerokości pasma sygnału.

Pojęcia podstawowe

Szyfrowanie - stosowane jest po to, aby zapewnić:

- ⇒ **poufność informacji (prywatność)**,
- ⇒ **autenticzność informacji (integralność)**.

Szyfrator ma za zadanie tak zmienić informację, aby była ona niezrozumiała dla osoby nieuprawnionej do odczytania wiadomości. Odtworzenie jawnej treści informacji następuje dopiero w **deszyfratorze**, którego zadaniem jest również stwierdzenie czy wiadomość jest autentyczna.

Szyfrowanie nie zwiększa ilości bitów w informacji.

Pojęcia podstawowe

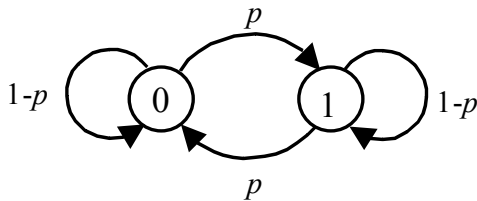
Modulacja – nadanie sygnałowi elektrycznemu cech charakterystycznych w celu przesłania informacji.

Modulator odwzorowuje zbiór symboli (słów binarnych) na zbiór sygnałów odpowiednich do przesłania w medium transmisyjnym.

Demodulator przeprowadza demodulację i detekcję odebranych sygnałów. Podejmuje decyzję, który symbol (słowo binarne) zostało nadane.

Dyskretne kanały bez pamięci

W kanale sygnałowym bez pamięci wyjście detektora w określonym przedziale czasu zależy jedynie od sygnału wysłanego w tym przedziale i nie zależy od sygnałów wysyłanych uprzednio



p - jest prawdopodobieństwem warunkowym $p(i/j)$ odbioru symbolu j w założeniu, że wysłano przez kanał symbol i .

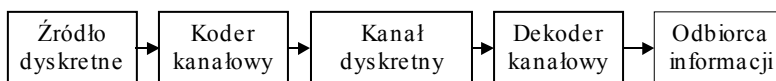
Najprostszy dyskretny kanał bez pamięci otrzymujemy stosując binarne symbole wejściowe i wyjściowe. Przy kodowaniu binarnym na wejściu modulatora pojawiają się symbole binarne „0” i „1”.

Robert Borowiec

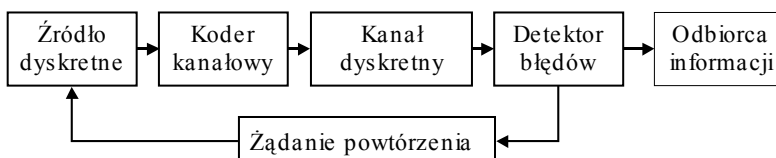
Kryptografia, Wykład I,
Systemy cyfrowe, strona 11/13

Poprawa jakości transmisji

Korekcja błędów w przód



Automatyczne żądanie powtórzenia



Robert Borowiec

Kryptografia, Wykład I,
Systemy cyfrowe, strona 12/13

Podział kodów

➤ W ujęciu historycznym kody dzieli się na:

- ☒ blokowe
- ☐ splotowe

Kodowanie blokowe polega na wprowadzeniu na wejście kodera bloków informacji binarnej o długości k bitów i dodaniu do nich $n-k$ bitów nadmiarowych (parzystości).

Przy *kodowaniu splotowym* informacja bitowa z wejścia jest przetwarzana w sposób ciągły. Koder dokonuje dyskretnego splotu strumienia informacji bitowej z odpowiedzią impulsową kodera.

KONIEC

Dziękuję za uwagę