

In our discussion of radio transmissions in this class we've considered all transmissions to be of a fixed frequency – or at least having a fixed carrier frequency. This is fine for most uses. For example, it's very convenient and cheap to have an FM radio station broadcast itself at a known carrier frequency. Listeners can simply tune in their radio and listen. But what if we want to transmit information but we don't want to broadcast ourselves to the world such that everybody can hear us?

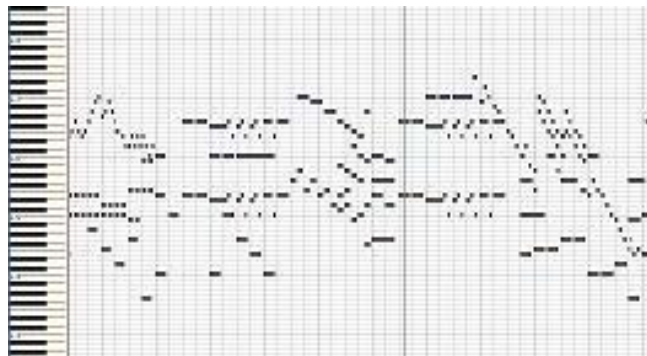
1. Brainstorm on some reasons why or situations in which we'd like to transmit information while making it hard for other people to snoop.
2. Better yet, what might be some advantages of transmitting data via radio in such a fashion that nobody even knows that you're transmitting? Anything specific to the military?

In this set of notes, we'll look at two methods for making it difficult for outsiders to listen in our on conversations: frequency-hopping spread spectrum and direct sequence spread spectrum. Although different in operation, both methods attempt to hide a transmission in a large chunk of the electromagnetic spectrum. The potential snooper is thwarted because they can't reliably find the transmission over such a large search area.

Frequency-Hopping Spread Spectrum

The idea behind frequency-hopping spread spectrum is to rapidly move the frequency of a transmission in a seemingly random fashion across a large range of the EM spectrum.

As an interesting aside, the idea was originally proposed and patented in 1942 by actress Hedy Lamarr and pianist George Antheil to protect torpedo guidance commands from jamming.



In a frequency hopping spread spectrum, the carrier frequency is switched in a **pseudorandom** fashion. A pseudorandom pattern is one that appears random (unpredictable) to the uniformed observer, but is in fact a predictable and reproducible. Of course for the system to work, the sender and receiver have to know the pattern and have synchronized timing so that they can switch to the right frequency at the right time. A simple illustration of the concept is shown in Fig. 1 below.

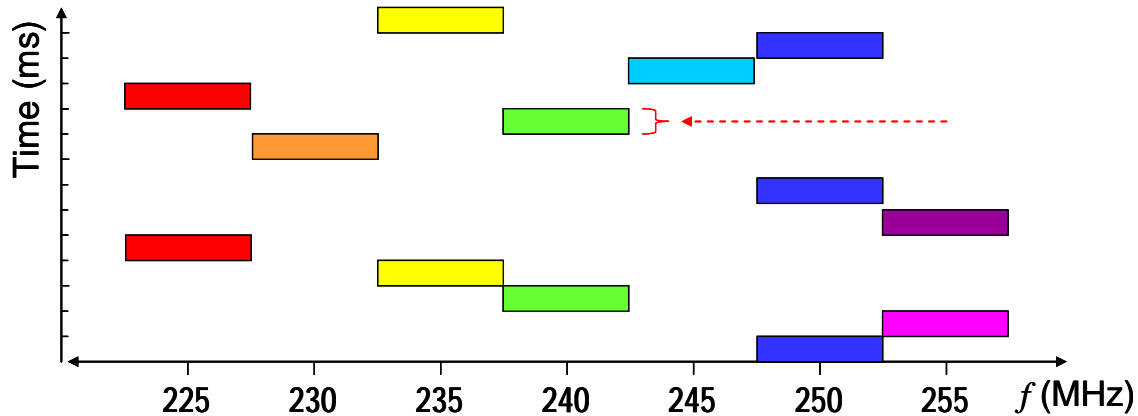


Figure 1. An example of frequency-hopping using seven frequency ranges.

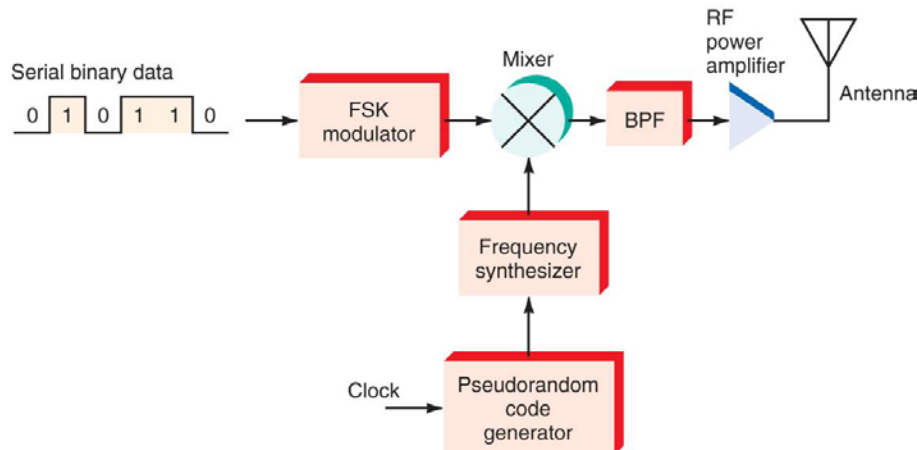


Figure 2. A high-level diagram of a frequency-hopping transmitter.

Figure 2 below shows a high-level description of a frequency-hopping transmitter. The transmitter modulates the binary data into an FSK signal. That FSK signal is then mixed with a pseudorandom frequency-hopping carrier signal. The mixed signal is then subjected to a band pass filter before being amplified and transmitted.

3. We saw a binary signal that was FSK modulated in a video the other day. What happened to the nature of the EM spectrum of the FSK signal as the bit rate increased?

EE 334
Wideband Modulation

Typically the rate of frequency change is much higher than the data rate. The illustration in Fig. 3 below shows a frequency synthesizer that changes 4 times for each data bit. Generally, the frequency changes faster than the baud. The time period spent on each frequency is called the **dwell time** (typically < 10 ms).

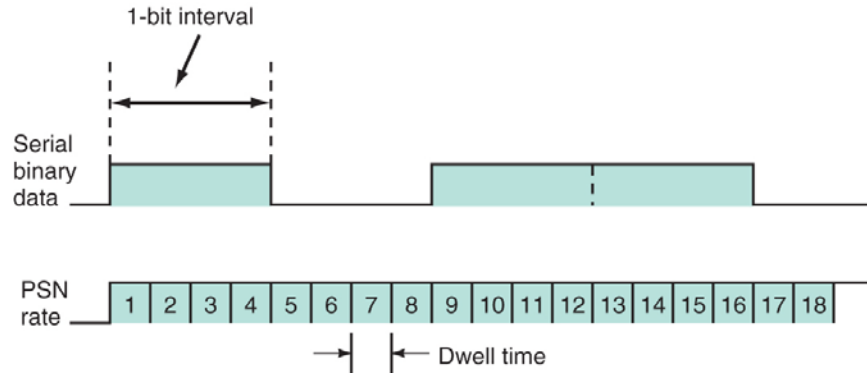


Figure 3. The frequency changes faster than the time to transmit a bit or baud in most frequency-hopping systems.

4. Why do we need a dwell time?
5. What's advantageous about changing frequencies at a faster rate than the baud?
6. If the frequency changes at a very high rate and is over a large enough range, what would someone "see" even if they were trying to snoop on the transmission?

The military uses frequency-hopping radios quite often. The SINCGARS is a VHF-FM frequency-hopping system used by the Army, Navy, and USMC. It operates on any or all of the 2,320 frequencies between 30 and 87.975 MHz in 25 kHz increments. HAVEQUICK is a frequency-hopping system used in aircraft radios to provide anti-jamming. HAVEQUICK radios are synchronized by a timing signal (usually GPS) and steps through a pre-determined set of frequencies which is loaded into the radio daily.

Direct Sequence Spread Spectrum

Another method of realizing spread spectrum is called **direct sequence spread spectrum (DSSS)**. In DSSS, the serial binary data is XORed with a pseudo-random binary code which has a bit rate faster than the binary data rate, and the result is used to phase-modulate a carrier. The bit rate of the pseudorandom code is called the **chipping rate**.

Sudden phase changes to a carrier signal (like those occurring in simple BPSK) cause the bandwidth of the resulting modulated signal to increase. Beyond that, if we increase the rate of the phase changes of the carrier the bandwidth also increases. If we can get the phase change rate up high enough (thanks to a high chipping rate), the resulting modulated signal will look more like noise than an actual signal. It would look like noise just from the rapid phase changes. However, it becomes even more noise-like due to the fact that the phase changes are generated in a pseudorandom fashion.

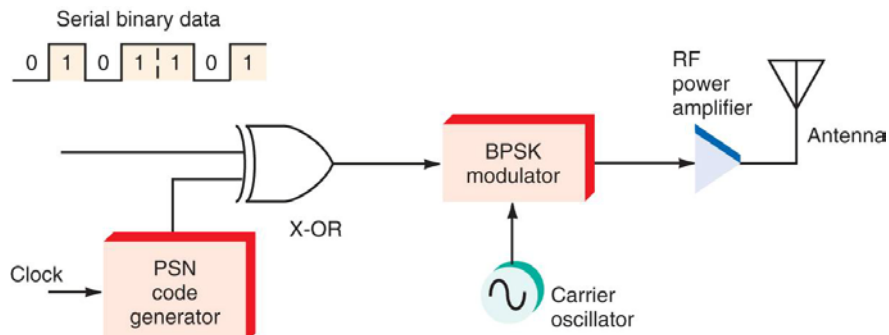


Figure 4. A high-level description of a DSSS system.

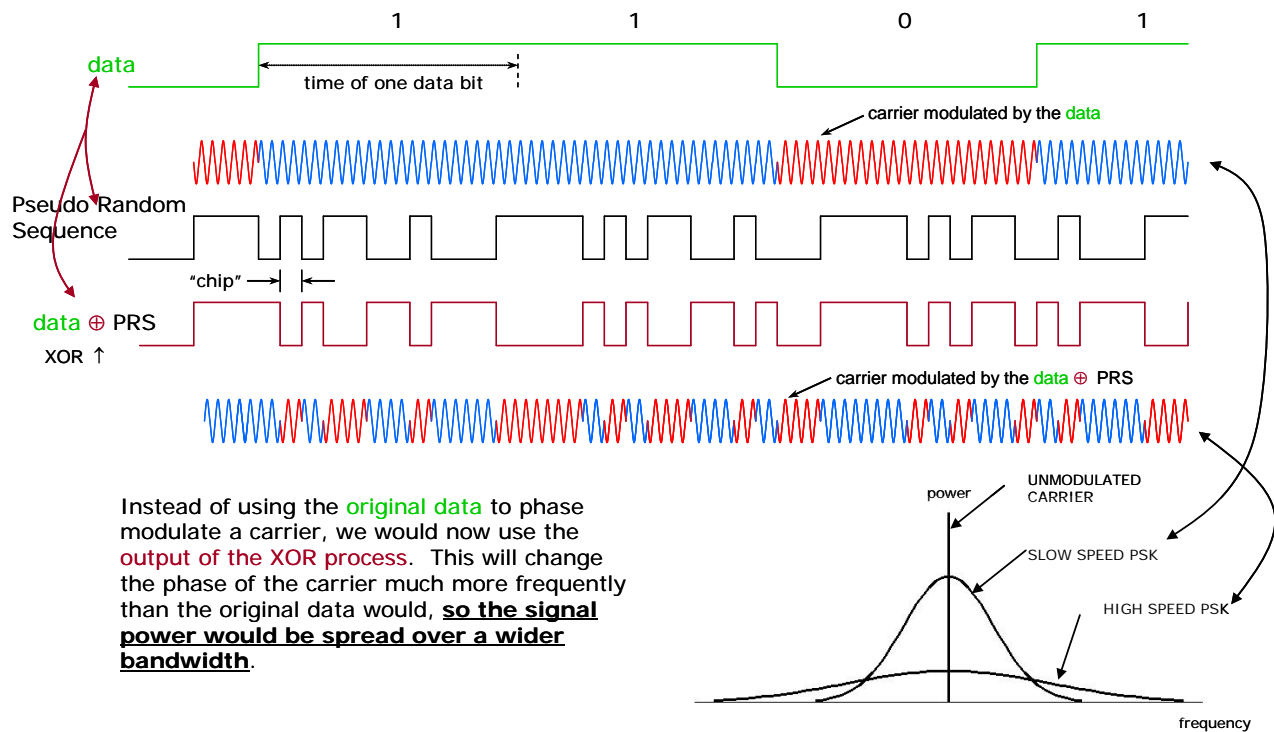


Figure 5. An illustration of the spread spectrum and noise properties of DSSS.

In DSSS, a signal that would normally occupy a few kHz of bandwidth (say like your regular FM broadcast) is spread out 10 to 10,000 times its normal bandwidth. The energy that would normally be concentrated in that narrow bandwidth is still there in DSSS, but has been spread out, too. In fact the energy is so spread out, that it's often indistinguishable from the normal atmospheric background noise as shown in Fig. 6 below. It's so diluted that it appears as noise in a conventional receiver. Recall problem #3 from a few pages ago where rapid frequency changes caused noise like effects and spreading of a signal's bandwidth.

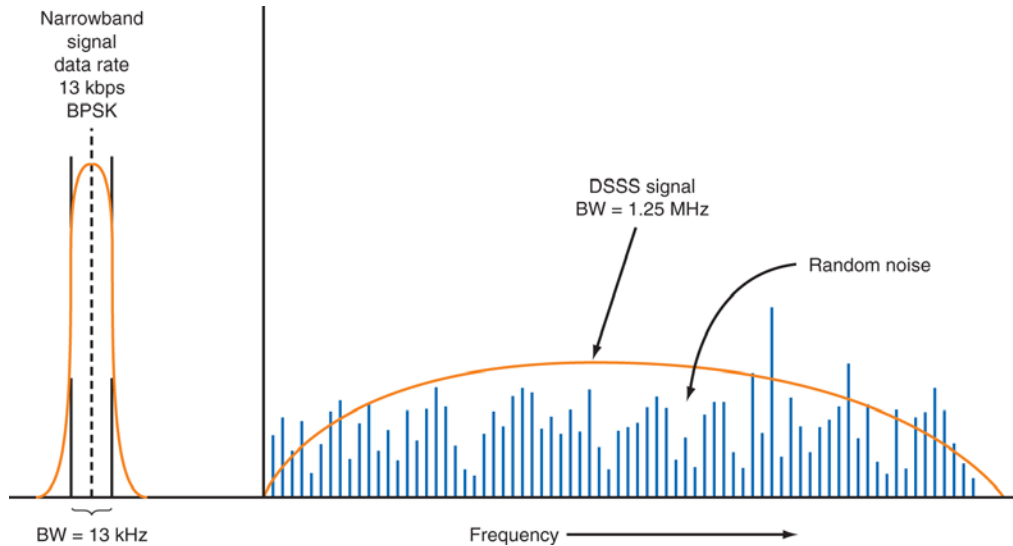


Figure 6. The energy of a DSSS signal is spread over such a large bandwidth that the energy is indistinguishable from naturally occurring background noise.

As was the case with frequency-hopping spread spectrum, a DSSS receiver must know the pseudorandom sequence of the transmitter and have a synchronizing circuit to get in step with this pseudorandom digital signal. The receiver using an identically programmed PN sequence can then “see” incoming matched signal clearly from the noise. Even cooler, multiple DSSS broadcasts can overlap each other spectrum-wise. Other signals using different PN sequences appear as noise to the receiver and is ignored.

DSSS is also called Code Division Multiple Access (CDMA). CDMA is used in satellites and digital cell phones.

7. List some reasons CDMA is attractive for cell phones and satellites.

The measure of the spreading is called the *processing gain*, G , which is the ratio of the DSSS bandwidth, BW , divided by the data rate, f_b .

$$G = \frac{BW}{f_b}$$

The higher the processing gain, the greater the DSSS signal's ability to fight interference.

8. A 13 kbps binary signal is spread over a bandwidth of 1.25 MHz using BPSK. What is the processing gain of the resulting DSSS signal? Express the answer as a ratio and in decibels.

Benefits of Spread Spectrum

Spread spectrum is being used in more and more applications in data communications.

- **Security** – need a wide BW receiver and precise knowledge and timing of the pseudorandom sequence
- **Resistance to jamming and interference** – jamming signals are usually restricted to one frequency
- **Band sharing** – many signals can use the same frequency band; but... many spread spectrum signals raise the overall background noise level
- **Resistance to fading** – fading is a frequency-selective phenomenon; a spread spectrum signal doesn't reside at only one frequency
- **Precise timing** – signals jump so quickly that even the most determined snooper will only "see" a fraction of a bit's worth of data

Pseudorandom Sequences

There are many ways to generate pseudorandom sequences. One way is with software algorithms that implement some mathematical formula that produces seemingly random patterns. These algorithms, while used widely and highly flexible, are relatively slow. They'd be hard pressed to keep up with the demands of frequency hopping or DSSS transmissions.

For high-speed pseudorandom numbers, hardware solutions are the way to go. Pseudonoise (PN) generators that can produce a seemingly random stream of 0s and 1s can be easily built from XOR gates and flip-flop shift registers. Together, they form a kind of state machine called a **linear feedback shift register (LFSR)**.

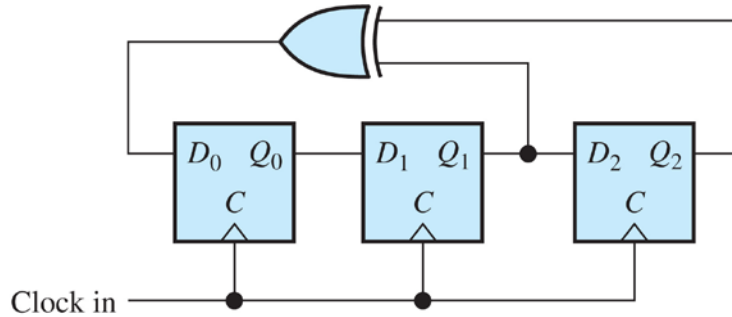


Figure 7. A PN state machine.

9. Draw the timing diagram for the PN state machine shown in Figure 7. The initial state of the machine is $Q_0 = 1, Q_1 = Q_2 = 0$.

10. Assuming Q_2 is the output of the state machine, write down the pseudorandom sequence of bits produced.

11. The state machine in Figure 7 is typical of PN generators in terms of the maximum number of bits it can produce before the pseudorandom sequence begins to repeat. How many bits were produced by this state machine before the pattern started to repeat?

12. Write down a general formula for the maximum sequence length of a PN generator having n flip-flops.

maximum sequence length =

EE 334
Wideband Modulation

In practice, we can leave the flip-flops in a shift register configuration but change the way in which the various stages are XORd together. For every logic combination of the XORs we realize a different PN sequence. If n is the number of flip-flops in use, the bounds on the number of possible sequences, S , is given by.

$$2^n - 1 \geq S \geq \frac{4(2^n - 1)}{15n} \approx \frac{(2^n - 1)}{4n}$$

13. How long is the maximal sequence for an LFSR having 32 flip-flops?

14. What is the lower bound on the number of possible maximal length sequences for an LFSR having 32 flip-flops?

15. What is the implication of the above two problems for someone trying to listen into your spread spectrum conversation? Do you feel secure? How can you increase your security?