# MATH-314 notes 9/12/2017

## One-Time Pad cipher

Choose a key that is a random string of letters the same length as the plaintext.
Encryption is then exactly the same as a vigenere cipher.
One-time pad is a perfect cryptosystem, meaning it has "perfect secrecy"

### Example:

Suppose Eve intercepts the message "SBY".
She knows that Alice and Bob are using a one-time pad cipher. Could the plaintext have been "CAT"? If the key was $< 16, 1, 18 >$, then yes. In fact, it could be any three letter word. But that doesn't really tell us anything.

## Conditional Probability

$P(A)$ = the probability that $A$ occurs.
$P(A|B)$ = the probability that $A$ occurs if $B$ has occurred.
The formula for conditional probability is:

$$P(A|B) = \frac{P(A \wedge B)}{P(B)}$$

### Example:

Suppose we observe the weather in Towson. We make a table of the probabilities that the weather in the morning and afternoon will be certain ways.

| | | Morning | | | |
|---|---|---|---|---|---|
| | | Sunny | Rainy | Snowy | |
| Afternoon | Sunny | $\frac{1}{5}$ | $\frac{1}{10}$ | 0 | $\frac{3}{10}$ |
| | Rainy | $\frac{1}{10}$ | $\frac{1}{5}$ | $\frac{1}{10}$ | $\frac{4}{10}$ |
| | Snowy | 0 | $\frac{1}{10}$ | $\frac{1}{5}$ | $\frac{3}{10}$ |
| | | $\frac{3}{10}$ | $\frac{4}{10}$ | $\frac{3}{10}$ | |

What is the probability that it is sunny in the morning?
Adding up the probabilities $\frac{1}{5}$ and $\frac{1}{10}$ gives us: $P(\text{sunny morning}) = \frac{3}{10}$

Suppose it is rainy in the morning. What is the probability that it will be sunny in the afternoon?

$$P(\text{sunny afternoon}|\text{rainy morning}) = \frac{P(\text{sunny afternoon} \wedge \text{rainy morning})}{P(\text{rainy morning})}$$

$$= \frac{\frac{1}{10}}{\frac{4}{10}} = \frac{1}{4}$$

# Perfect Secrecy

Say that a cryptosystem has perfect secrecy if for every key $k$ and every ciphertext $c$ and plaintext $p$:

$$P(\text{plaintext is } p) = P(\text{plaintext was } p | \text{ciphertext is } c)$$

Meaning Eve does not learn anything by learning the ciphertext.

## Example:

Alice and Bob want to send either `yes` or `no`. The use a cryptosystem with 3 keys - $k_1, k_2, k_3$ - one of which they pick at random for each message.

| | $k_1$ | $k_2$ | $k_3$ |
|---|---|---|---|
| `yes` | 1 | 2 | 3 |
| `no` | 2 | 3 | 4 |

Eve knows that alice and bob send `yes` $\frac{1}{4}$ of the time and `no` $\frac{3}{4}$ of the time.
First eve captures the ciphertext 3 (she doesn't know what key Bob and Alice are using). What is the probability that the message was `yes`?

$$P(p = \texttt{yes}) = \frac{1}{4}$$

$$P(p = \texttt{yes} | c = 3) = \frac{P(p = \texttt{yes} \wedge c = 3)}{P(c = 3)}$$

$$= \frac{P(p = \texttt{yes} \wedge k = k_3)}{P(c = 3)}$$

$$= \frac{P(p = \texttt{yes}) \times P(k = k_3)}{P(c = 3)}$$

$$= \frac{\frac{1}{4} \times \frac{1}{3}}{P(p = \texttt{yes} \wedge k = k_3) \vee P(p = \texttt{no} \wedge k = k_2}$$

$$= \frac{\frac{1}{12}}{\frac{1}{4} \times \frac{1}{3} + \frac{3}{4} \times \frac{1}{3}} = \frac{1}{4}$$

Which is the same as $P(p = \texttt{yes})$. So eve didn't learn anything from this.
However, this system still may not have perfect secrecy. What if $c = 1$?

$$P(p = \texttt{yes}) = \frac{1}{4}$$

$$P(p = \texttt{yes} | c = 1) = 1$$

These are not equal, so Eve did learn something and this cryptosystem does not have perfect secrecy.

The one-time pad has perfect secrecy.

Proof (sort of): any ciphertext can be produced by any plaintext with exactly one key and every possible key is equally likely to have been chosen.

Disadvantages of the one-time pad:

Both Alice and Bob need to already share a key

The key has to be as long as the plaintext, so transmitting the key is just as difficult as transmitting the plaintext.

The key cannot be used more than once.

This system is just not practical in most circumstances.