NOTES ON SHANNON'S THEOREM
MATH/CMSC 456

PROF. JONATHAN ROSENBERG
SPRING 2009

Since this material is not in the text in the form we were discussing, here are some notes on Shannon's theory of perfect security. We assume we are dealing with a private-key encryption system with a set $\mathcal{K}$ of possible keys, a set $\mathcal{M}$ of possible messages, and a set $\mathcal{C}$ of possible ciphertexts. We assume that a key K is chosen from the set $\mathcal{K}$ according to a certain probability distribution, and a message M is chosen from the set $\mathcal{M}$ with another probability distribution. The "encryption machine" then produces from this data a ciphertext $C(M, K) \in \mathcal{C}$. Note that the probability distributions on $\mathcal{K}$ and $\mathcal{M}$ define one on $\mathcal{C}$, since the ciphertext is a function of the message and the key. For simplicity (so we never have to worry about dividing by zero), let's assume each element of $\mathcal{K}$, $\mathcal{M}$, and $\mathcal{C}$ has positive probability. (Otherwise just throw away the elements with probability 0.) We denote probabilities by $P(\_\_)$, conditional probabilities by $P(\_\_ \mid \_\_)$.

Definition 1 (Shannon, 1949)**.** The system is *perfectly secure* or *perfectly secret* if knowing the ciphertext gives no more information about the message that one would know without intercepting the encoded message at all, or in other words, if $P(M = m) = P(M = m \mid C = c)$ for any $c \in \mathcal{C}$ and any $m \in \mathcal{M}$, regardless of what probability distribution is chosen on $\mathcal{M}$. As we saw in class, this is equivalent to saying that $P(C = c) = P(C = c \mid M = m)$ for any c and m.

This definition would be useless if there were no examples satisfying it, but fortunately we have:

Theorem 1. *The one-time pad is perfectly secure.*

Proof. Recall the way this works: we fix a message length n and assume $\mathcal{K} = \mathcal{M} = \mathcal{C} = \{\text{all sequences of } n \text{ bits}\}$. We choose the key according to the *uniform* distribution, so all keys are equally likely (with probability 2^{-n}). Then given that the message is $M = m$ and the key is $K = k$, the ciphertext is $c = m \oplus k$, and we decode using the same key: $m = c \oplus k$. Note that the key and the message are chosen totally independently of one another, so regardless of what the message is,

all ciphertexts are equally likely with probability 2^{-n}. In other words, regardless of c and m, $P(C = c) = P(C = c \mid M = m) = 2^{-n}$, so we have perfect security. □

This raises the question of what other systems can satisfy the definition. Unfortunately, it turns out that for perfect security, the key has to be as long as the message, and the system has to be very much like a one-time pad!

Theorem 2. *Suppose an encryption system as above is perfectly secure. Then the set $\mathcal{K}$ of possible keys must be as big as the set $\mathcal{M}$ of possible messages.*

Proof. Suppose not, i.e., $|\mathcal{M}| > |\mathcal{K}|$. If we fix a ciphertext $c \in \mathcal{C}$, there are at most $|\mathcal{K}|$ possible decodings of c, and since $|\mathcal{M}| > |\mathcal{K}|$, there must be a message m that cannot encode to c. Thus for this choice of m, $P(M = m \mid C = c) = 0$. Since we are assuming that $P(M = m) > 0$ for all $m \in \mathcal{M}$, $P(M = m \mid C = c) \neq P(M = m)$, contradicting perfect security. □

Theorem 3 (Shannon, 1949)**.** *Assume we have an encryption system as above and the sets $\mathcal{K}$, $\mathcal{M}$, and $\mathcal{C}$ all have the same size. Then*

1. *Each key must be chosen with equal probability $\frac{1}{|\mathcal{K}|}$.*
2. *For every message $m \in \mathcal{M}$ and every possible ciphertext $c \in \mathcal{C}$, there must be a unique key k such that $C(m, k) = c$.*

Proof. Part of (2) is like the last theorem — if we are given m and c and no key k satisfies $C(m, k) = c$, then $P(M = m \mid C = c) = 0 \neq P(M = m)$. Similarly, if two keys k_1 and k_2 satisfy $C(m, k_1) = C(m, k_2) = c$, then since there were only as many keys as ciphertexts, there must be another ciphertext c' with $C(m, k) \neq c'$ for all k, and the same argument applies again. So this verifies (2).

Now we assume (2) and prove (1). Suppose there are two keys k_1 and k_2 with $P(k_1) > P(k_2)$. Fix m and let $C(m, k_1) = c_1$, $C(m, k_2) = c_2$. Then $P(M = m \mid C = c_1) = P(k_1) > P(k_2) = P(M = m \mid C = c_2)$ (since by (2), k_1 and k_2 are the unique keys coding m to c_1 and c_2, respectively). Thus we cannot have perfect security, which would require $P(M = m \mid C = c_1) = P(M = m \mid C = c_2) = P(M = m)$. This contradiction proves (1). □