

Math 400 Fall 2017
Cryptology HW 4 Solutions
Due Thursday, September 28

1. Consider a cipher with three keys, three plaintexts, and four ciphertexts, given by:

$$\begin{array}{c} k_1 \\ k_2 \\ k_2 \end{array} \left\| \begin{array}{c|c|c} m_1 & m_2 & m_3 \\ \hline c_2 & c_4 & c_1 \\ \hline c_1 & c_3 & c_2 \\ \hline c_3 & c_1 & c_2 \end{array} \right.$$

Suppose all keys are equally likely, and the messages have probability $P(m_1) = 2/5$, $P(m_2) = 2/5$, $P(m_3) = 1/5$.

- (a) What is the probability of each ciphertext?
- (b) Compute $P(c_1|m_1)$, $P(c_1|m_2)$, $P(c_1|m_3)$. Can you tell if the ciphertext has perfect secrecy?
- (c) Compute $P(c_2|m_1)$, $P(c_3|m_1)$, $P(c_4|m_1)$.
- (d) Compute $P(k_1|c_3)$, $P(k_2|c_3)$, $P(k_3|c_3)$.

Solution:

- (a) $P(c_1) = 1/3$, $P(c_2) = 4/15$, $P(c_3) = 4/15$, $P(c_4) = 2/15$.
 - (b) $P(c_1|m_1) = 1/3$, $P(c_1|m_2) = 1/3$, $P(c_1|m_3) = 1/3$. This doesn't tell us if we have perfect secrecy. (It doesn't prove we *don't*, but we'd need to check for all $c \in \mathcal{C}$ to be sure).
 - (c) $P(c_2|m_1) = 1/3$, $P(c_3|m_1) = 1/3$, $P(c_4|m_1) = 0$. Thus we don't have perfect secrecy, since the ciphertext constrains the message.
 - (d) $P(k_1|c_3) = 0$, $P(k_2|c_3) = 1/2$, $P(k_3|c_3) = 1/2$.
2. Suppose $\#\mathcal{M} = \#\mathcal{C}$. Prove that for a fixed key $k \in \mathcal{K}$ and a fixed ciphertext $c \in \mathcal{C}$, there is a unique plaintext $m \in \mathcal{M}$ such that $e(k, m) = c$. (Hint: this is a counting argument using the fact that e_k is 1-1).

Solution: Fix $k \in \mathcal{K}$. Then the function $e_k : \mathcal{M} \rightarrow \mathcal{C}$ is injective, and an injection from one finite set to another is a bijection. Thus e_k is a bijection and thus invertible, and for every $c \in \mathcal{C}$ there is a unique $e_k^{-1}(c)$.

3. Let X be a random variable with possible outcomes x_1, \dots, x_n , and Y a random variable with possible outcomes y_1, \dots, y_m . Let Z be a random variable that corresponds to testing X followed by Y , so the possible outcomes are pairs (x_i, y_j) with $P(x_i, y_j) = P(x_i)P(y_j)$.

Use the definition of entropy to prove that $H(Z) = H(X) + H(Y)$. This is a special case of property 3 from Shannon's theorem.

Definition 0.1. The *Key Equivocation* of a cryptosystem is $H(K|C) = H(K) + H(M) - H(C)$. (There's a more complicated formula in terms of random variables, which I'm omitting here). It measures the amount of information about the key revealed by the ciphertext.

In particular, it tells us how much *more* information we get from the key if we already know the ciphertext. If it is low, knowing the ciphertext tells us a lot about the key. If it's zero, we can determine the key and message purely from the ciphertext.

4. Suppose we have a cryptosystem with two keys $\mathcal{K} = \{k_1, k_2\}$ and three plaintext $\mathcal{M} = \{m_1, m_2, m_3\}$. Suppose the plaintexts have probabilities $P(m_1) = 1/2, P(m_2) = P(m_3) = 1/4$.

- Create an encryption function with three ciphertexts $\mathcal{C} = \{c_1, c_2, c_3\}$, such that $P(c_1) = 1/2$.
- Compute $H(K), H(M), H(C)$.
- Compute the equivocation $H(K|C)$.
- How secure is this cipher?

5. How does key equivocation relate to unicity distance?

Solution: Unicity distance is the message length at which you expect to have a 50% chance of completely decrypting the ciphertext without any additional info; so it's the distance where you expect the key equivocation to be close to zero. With much shorter messages the key equivocation will be high; with much longer messages, the key equivocation will be zero.

Note that the unicity distance isn't deterministic, so we can't say that the equivocation is zero any time the message length is over the unicity distance.

6. Compute the unicity distance for

- An autokey cipher
- A Hill cipher with a block size of 2
- A Hill cipher with a block size of 5.

Solution:

- If the key word has length N then there are 26^N possible keys, which is $4.7N$ bits of entropy. We divide by 3.2 to get a unicity distance of $1.47N$.
- There are 26^4 possible matrices, but only $12/26$ of them will be invertible. So there are $26^3 \cdot 12$ possible keys, which is 17.7 bits of entropy. We divide by 3.2 to get 5.5.

- (c) There are 26^{25} matrices and again only $12/26$ will work. So there are $26^{24} \cdot 12$ possible keys, which corresponds to about 116.4 bits of entropy. Dividing by 3.2 gives a unicity distance of 36.4.