

Cryptography – E16 – Lecture 3

Lecture, September 6

We covered section 1.1 on algebra. There are more notes on this on the course homepage, along with some slides. In the discrete math notes, algebra starts on page 6. In addition, you should read about the Extended Euclidean Algorithm and the Chinese Remainder Theorem (section 1.3 in the textbook) if you are not familiar with them or need a review.

Lecture, September 12

We will cover chapter 9 and section 11.2, including the proof of Lemma 2.3 and the birthday bound at the top of page 24.

Lecture, September 14

We will cover sections 11.5 and 12.2 and then briefly discuss the remainder of chapter 12. We may then begin on chapter 13.

Problem session September 19

1. Suppose a cryptosystem achieves perfect security for a particular plaintext probability distribution. Prove that perfect secrecy is maintained for any plaintext probability distribution. (This was problem 2.4 in the textbook, *Cryptography: Theory and Practice*, by Stinson, 3rd edition (CTP).)
2. Prove that $H(X, Y) = H(Y) + H(X|Y)$. Then show as a corollary that $H(X|Y) \leq H(X)$, with equality if and only if X and Y are independent. (Problem 2.10 in CTP.)

3. Prove that a system has perfect secrecy if and only if $H(P|C) = H(P)$. (Problem 2.11 in CTP.)
4. Let $m \geq 1$ be an integer. The m -gram Substitution Cipher is the substitution cipher where the plaintext (and ciphertext) spaces consist of all 26^m m -grams (m consecutive letters). Estimate the unicity distance of the m -gram Substitution Cipher if $R_L = 0.75$. (Problem 2.17b in CTP.) You may use the approximation that $\log_2(n!) \approx \log_2(e)((n+1)\log_e(n+1) - n)$; this is an upper bound. How does this approximation work for the case $m = 1$ and $m = 2$?
5. Suppose a cryptosystem has $P = \{a, b, c\}$, $C = \{1, 2, 3, 4\}$ and $K =$

| | | | |
|-------|-----|-----|-----|
| | a | b | c |
| k_1 | 1 | 2 | 3 |
| k_2 | 4 | 3 | 2 |
| k_3 | 3 | 4 | 1 |

$\{k_1, k_2, k_3\}$. The encryption rules are as follows:

Suppose $p(K = k_i) = 1/3$ for $1 \leq i \leq 3$, $p(P = a) = 1/2$, $p(P = b) = 1/3$, and $p(P = c) = 1/6$.

- a. Compute the probabilities $p(C = y)$ for all $y \in \{1, 2, 3, 4\}$.
 - b. Does this cryptosystem achieve perfect secrecy? Explain your answer.
6. I may lecture at the end.