Homework 1

Due: September 20, 2024

CS 1510: Intro. to Cryptography and Computer Security

1 Cryptanalysis

One of the oldest known ciphers is the shift cipher or Caesar cipher, which simply shifts each letter in the message forward in the alphabet by some fixed number of steps. For example, shifting each letter forward by 3 turns ONETIMEPAD into RQHWLPHSDG. Of course this cipher only has 26 possible keys (and one leaves the original message unchanged), so it is easy to just try every possibility. It would be better to use a different shift for each letter, to increase the number of possible keys. We can represent such a key using letters of the alphabet so that A represents a shift by 0, B represents a shift by 1, etc. So using the key EXAMPLEKEY we can encrypt ONETIMEPAD to SKEFXXIZEB.

a. Everyone knows that Alice and Bob have a far from perfect relationship. Alice loves Bob a third of the time and hates him otherwise. Bob loves Alice half the time and hates her a quarter of the time; the rest of the time he is watching football. Oddly enough, these events seem to be independent.

When they realized that their friends were putting odds on their emotional states, Alice and Bob started using the cipher above to preserve their privacy. When appropriate they send each other messages saying either "I love you" or "I hate you." When Bob is watching the game, he sends random letters in the same word pattern (e.g., "Z wtrh bah").

The following is a transcript of Alice and Bob's messages for the last few days. The encryption leaves spaces, punctuation, and capitalization the same as in the original text. What key or keys have they been using, and at what times? How can you tell?

Saturday, 7:45am Alice \rightarrow Bob: J fube zci Saturday, 8:11am Bob \rightarrow Alice: J fube zci Saturday, 11:27am Bob \rightarrow Alice: J bgze zci Saturday, 12:34pm Alice \rightarrow Bob: J bgze zci Saturday, 3:06pm Alice \rightarrow Bob: J bgze zci Saturday, 7:59pm Bob \rightarrow Alice: J fube zci Sunday, 1:19am Bob \rightarrow Alice: J fube zci

Sunday, 5:23am Alice \rightarrow Bob: J bgze zci Sunday, 1:47pm Bob \rightarrow Alice: I kuna egw Sunday, 3:29pm Alice \rightarrow Bob: J fube zci Sunday, 5:18pm Alice \rightarrow Bob: P fubc zsy Sunday, 7:30pm Bob \rightarrow Alice: P bgzc zsy Sunday, 9:41pm Bob \rightarrow Alice: U ilol qim Monday, 4:55am Alice \rightarrow Bob: P bgzc zsy Monday, 7:11am Alice \rightarrow Bob: P bgzc zsy Monday, 11:11am Bob \rightarrow Alice: P fubc zsy Monday, 4:20pm Alice \rightarrow Bob: P bgzc zsy Monday, 10:36pm Bob \rightarrow Alice: P fubc zsy Monday, 11:58pm Alice \rightarrow Bob: U lhvl yfc Tuesday, 2:54am Bob \rightarrow Alice: U httl yfc Tuesday, 6:47am Bob \rightarrow Alice: U lhvl yfc Tuesday, 8:51am Alice \rightarrow Bob: U httl yfc Tuesday, 9:13am Alice \rightarrow Bob: U httl yfc Tuesday, 9:56am Bob \rightarrow Alice: U lhvl yfc Tuesday, 10:29am Alice \rightarrow Bob: Mtmajk rb papn

b. Something weird is going on. Alice's last message to Bob was not what you expected. Are Alice and Bob secretly working for your archnemesis, the evil Peihan? If so, your life could already be in danger. If something happens to you, your best friends, Carol and Dave, need a way to decrypt the information on your laptop that will help them discover the truth about Alice and Bob. You want to make sure they are together when they read the information, just in case it is dangerous.

Your laptop is locked by a password K (for simplicity, assume K consists only of capital letters 'A'-'Z'). Building on the cipher above, explain how to generate a pair of messages, C and D to Carol and Dave respectively, such that, when put together, can reveal the password K for your laptop, but given just C or just D, no information about K (except its length) is revealed.

Extra credit: How would you break the secret K into more than two pieces?

c. It is true, Alice and Bob are evil spies! While attending a party at their house you managed to quietly slip away from the crowd to look for evidence. But when you found the weapon hidden behind the toilet you panicked, and Alice caught you sending your lawyer Trent an urgent warning using her computer. Luckily, you did

the encryption in your head, enciphering "Alice and Bob are evil" using your distress key, "QJDLEWOZMCVPWJHGSE." As a result, Alice's computer only logged the ciphertext. How can you convince her that you actually said, "Alice and Bob are nice"?

2 Perfect Security

Recall the definition of perfect security for a symmetric-key encryption scheme.

Definition 1 (Perfect Security) A symmetric-key encryption scheme (Gen, Enc, Dec) with message space \mathcal{M} is perfectly secure if for all probability distributions over \mathcal{M} , all messages $m \in \mathcal{M}$, and all ciphertexts $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$,

$$\Pr[M = m \mid C = c] = \Pr[M = m].$$

a. Consider the following definition:

Definition 2 (A Security) We say (Gen, Enc, Dec) is A-secure if for all distributions over \mathcal{M} , all $m \in \mathcal{M}$, and all $c \in \mathcal{C}$ for which $\Pr[M = m] > 0$,

$$\Pr[C = c] = \Pr[C = c \mid M = m].$$

Is A-security equivalent to the original perfect security definition? Prove or disprove your answer.

b. Consider another definition:

Definition 3 (B Security) We say (Gen, Enc, Dec) is B-secure if for all pairs of messages $m_0, m_1 \in \mathcal{M}$, and all $c \in \mathcal{C}$ for which $\Pr[M = m_0] > 0$ and $\Pr[M = m_1] > 0$,

$$\Pr[C = c \mid M = m_0] = \Pr[C = c \mid M = m_1].$$

Is B-security equivalent to the original perfect security definition? Prove or disprove your answer.

c. Alice and Bob are arguing in class. Bob insists that an encryption scheme with message space \mathcal{M} is perfectly secure if and only if for every probability distribution over \mathcal{M} and every pair of ciphertexts $c_0, c_1 \in \mathcal{C}$, it is the case that any computed ciphertext C must be equally likely to be c_0 or c_1 , i.e. that $\Pr[C = c_0] = \Pr[C = c_1]$. If you think Bob is correct, help him out by writing a proof of the statement. Otherwise, help Alice convince him that he is wrong by providing a counterexample.

3 One-Time Pad

Consider using a one-time pad with a randomly selected key $k = 0^{\ell}$, i.e. the all-zero string.

- a. What happens when we encrypt a message m using k?
- b. Carol proposes modifying the one-time pad by encrypting only with a key $k \neq 0^{\ell}$ (i.e. Gen only selects keys uniformly from the set of *non-zero* keys of length ℓ). Is Carol's proposed scheme perfectly secure? Why or why not?
- c. Some cryptographers might argue that as long as the encryption scheme is perfectly secure, sending a message using key $k = 0^{\ell}$ does not give the adversary any more information than they started with. Do you think this true in practice? Discuss.

4 Negligible Functions

In cryptography, we usually define security by requiring that the probability of some undesirable event (such as Eve guessing a message) be so small that no one would ever notice it. To that end, we define a negligible function as follows:

Definition 4 (Negligible function) A function $\nu(k) : \mathbb{N} \to [0,1]$ is negligible if for every polynomial p, there exists some $k_0 \ge 1$ such that for all $k > k_0$, $\nu(k) < |1/p(k)|$.

In this problem, we will develop some intuition for this concept and how to use it.

- a. Give an example of a negligible function $\nu(k)$ where $\nu(k) > 0$ for all k.
- b. Suppose that ν is a negligible function. Let p be a polynomial such that $p(k) \ge 0$ for all k > 0. Which of the following functions are necessarily negligible? For each function you think is necessarily negligible, provide a proof. For each you do not think is necessarily negligible, provide a counterexample.
 - (1) $\nu(k) \cdot p(k)$
 - (2) $\frac{1}{p(k)} \nu(k)$
 - (3) $\nu_1(k) \cdot \nu_2(k)^{-1}$ where both ν_1 and ν_2 are negligible
 - (4) $\nu(k)^{-c}$ for a positive constant c
 - (5) $\sum_{i=1}^{p(k)} \nu_i(k)$, where for all $i, k, \nu_i(k) \le \nu(k)$
- c. Suppose that $\varepsilon : \mathbb{N} \to [0,1]$ is not a negligible function. Is the following statement true: There exists a polynomial p where p(k) > 0 for all k, and some $k_0 \ge 1$, such that $\varepsilon(k) > 1/p(k)$ for all $k > k_0$. In other words, is ε necessarily asymptotically greater than some inverse polynomial? If you think the statement is true for every non-negligible function ε , prove it. Otherwise, provide a counterexample.

5 Summary Question

Summarize the most important insights from this week's material, including from the lectures, notes, textbooks, homework problems, and other resources you find helpful, into a one-page resource. We expect that these summary pages will help you with the take-home midterm and final. Please note this question is graded based on completion—we will not be checking it for correctness.