CS310 Cryptography **Handout # 8**
Randy Shull **September 22, 2016**
Wellesley College

Problem Set 4

Due: Start of Class, September 29, 2016

Overview: You may have noticed that our definitions of security assume all messages have the same length. Pretty clearly this is not the case. Fortunately, there is a simply remedy. In this exercise set your are asked to come up with one. You will also investigate the existence of pseudorandom functions as discussed in lecture.

Finally, you are asked to formulate a notion of perfect secrecy against chosen-plaintext attacks. Sadly, reasonable analogues of perfect secrecy cannot be achieved in the presence of chosen-plaintext attacks. We compare the notion of indistinguishable multiple encryptions in the presence of eavesdropper to schemes secure against chosen-plaintext attacks.

Reading:

- Sections 3.3, 3.4, 3.5 Katz and Lindell *Introduction to Modern Cryptography*

Problem 1 [6]: Indistinguishable encryptions in the presence of eavesdropper

Say $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is such that for $k \in \{0,1\}^n$, algorithm Enc_k is only defined for messages of length at most $\ell(n)$ (for some polynomial ℓ). Construct a scheme satisfying Definition 3.8 even when the adversary is not restricted to output equal-length messages in experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$. Justify your construction. You need not give a formal proof.

Discussion: To be clear, we are considering a modification of experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ where the adversary $\mathcal{A}$ is not required to output m_0 and m_1 of the same length, but instead it is only required that m_0 and m_1 each have length at most $\ell(n)$. Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a scheme that is secure with respect to the original Definition 3.8 (for messages of equal length). Construct a scheme $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ from Π that satisfies Definition 3.8 for message of unequal length.

Problem 2 [8]: Pseudorandom number generators

Let G be a pseudorandom generator where $|G(s)| > 2 \cdot |s|$.

1. Define $G'(s) \stackrel{\text{def}}{=} G(s||0^{|s|})$. Is G' necessarily a pseudorandom generator?

2. Define $G'(s) \stackrel{\text{def}}{=} G(s_1 \dots s_{n/2})$, where $s = s_1 \dots s_n$. Is G' necessarily a pseudorandom generator?

Problem 3 [Extra Credit 8]: Perfect secrecy against chosen-plaintext attack

Define a notion of perfect secrecy against a chosen-plaintext attack via the natural adaptation of Definition 3.22. Show that the definition cannot be achieved.

Discussion: Your definition will probably refer to the experiment $\mathsf{PrivK}^{\mathsf{cpa}}$ in Section 3.4. Let n be the security parameter and let $p(\cdot)$ be a polynomial such that Enc uses $p(n)$ random coin tosses to encrypt a message of length n. We construct an adversary A who receives input 1^n, outputs a pair of messages $m_0 = 0^n$ and $m_1 = 1^n$, and receives back the challenge ciphertext c. A then proceeds to query its encryption oracle $2^{p(n)}$ times with 0^n. If A receives c in response to one of these queries, then A outputs $b' = 0$; otherwise it outputs $b = 1$. Your job is to analyze A's probability of success. Although it may not be obvious at the moment, Proposition A.2 from Appendix A will be helpful here.

Problem 4 [4]: Indistinguishable multiple encryptions in the presence of eavesdropper

Assuming the existence of a pseudorandom function, show that there exists an encryption scheme that has indistinguishable multiple encryptions in the presence of an eavesdropper (i.e., is secure with respect to Definition 3.19), but is not CPA-secure (i.e., is not secure with respect to Definition 3.22).

Discussion: Your scheme need not be realistic. The goal here is to show that indistinguishable multiple encryptions in the presence of an eavesdropper does not imply CPA-secure. Devise a scheme that allows the adversary $\mathcal{A}$ to discover the key if $\mathcal{A}$ could ask the "right" questions, but for which "just listening in" is not enough.

Problem 5 [6]: Pseudorandom functions and CPA-secure

Let F be a pseudorandom function, and G a pseudorandom generator with expansion factor $\ell(n) = n + 1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. In each case, the shared key is a random $k \in \{0,1\}^n$. Justify your answers.

1. To encrypt $m \in \{0,1\}^{n+1}$ choose a random $r \leftarrow \{0,1\}^n$ and send $\langle r, G(r) \oplus m \rangle$.

2. To encrypt $m \in \{0,1\}^n$, send $m \oplus F_k(0^n)$.

3. To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 \parallel m_2$ with $|m_1| = |m_2|$, then choose $r \leftarrow \{0,1\}^n$ at random, and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.

Problem 6 [2]: Context-Free Grammars and Steganography Sending encrypted mail may keep the contents a secret, but in certain quarters it will raise red flags. Sometimes, knowledge that a communication took place at all, independent of its contents, is a problem. Steganography is the art of hiding messages in plain sight. When I was a kid we use lemon juice (which is very nearly clear and hence does not show on paper when dry) as an invisible ink. When heated, the lemon juice starts to burn and the released carbon shows up as brown writing on the page.

My friend Rhys Price-Jones wrote a Java program to hide images in the noise of other images. The color of each pixel in of an image represented in RGB scheme is represented as a 32-bit number. Each number is broken into four 8-bit components representing numbers between 0 and 255. The most significant eight bits represents the amount of transparency (with 255 fully opaque). The next eight bits is the intensity of the RED component of the color, the next the intensity of the GREEN component, and the least significant eight bits represent the intensity of the BLUE component.[1]

Think about the number representing the amount of each color: RED, GREEN, BLUE in each pixel. Do you think you could tell the difference if I changed it by a small number? Say change 132 to 128 Could you tell the difference between

```
RED 134, GREEN 156, BLUE 54
RED 129, GREEN 159, BLUE 57
```

By allowing changes just to the three rightmost bits the largest change you make to a single color component is a swing from $000_2(0_10)$ to $111_2(7_{10})$. Would you be able to tell if someone doctored an image by changing each color component within each pixel by a random amount that is at most 7 (7 out of 256 is about 3 percent). If, instead of changing randomly, what if someone changed in such a way that can convey information. That is exactly what Rhys did, in this case Rhys hide another image. This technique is known as *hiding in the noise*. Rhys's algorithm for hiding IMAGE1 in IMAGE2:

[1] Thus, you may start your Valentine Day poem for that special someone: Roses are #FF0000, violets are #0000FF...

1. Divide each of the color components of IMAGE1 by 32, yielding 3 most significant bits of that component.

2. Replace the three least significant bits of every component in IMAGE2 by the corresponding 3 bits from IMAGE1.

To retrieve Image1 reverse the steps:

1. Remove the 5 high order bits of every color component of IMAGE2.

2. Multiply the remaining three bits of each color component by 32 to obtain IMAGE1.

As an example, the figure on the left below is IMAGE2 (my friend Rhys) sent in the clear within which IMAGE1 (Rhys's dog Gruff) is hidden.


```
PicOps.display("mystery.txt")  > PicOps.display
                                    (PicOps.decode("mystery.txt"))
```

Figure 5.1. Gruff disguised as another.

If you compare the image of Gruff show here with the original you will see a significant loss of resolution due to the fact that only three bits of are used for each color component of each pixel. However, Gruff is quite recognizable.

The following questions explore other steganographic techniques.

1. Inspector Morse, whose abilities as crossword puzzler are legend had no difficulty discovering what it says. What does it say? For many years John Thaw played the quintessential Inspector Morse on BBC. In one of his cases, *The Silent World of Nicholas Quinn*, the good inspector uncovers the message shown in Figure 5.2 in which a subset of the words of the overall message is used to convey the hidden message. His trusty Watson (Sargent Lewis) is baffled, but Morse (being the

good crossword puzzler that he is immediately ferrets out the message. What does it say?

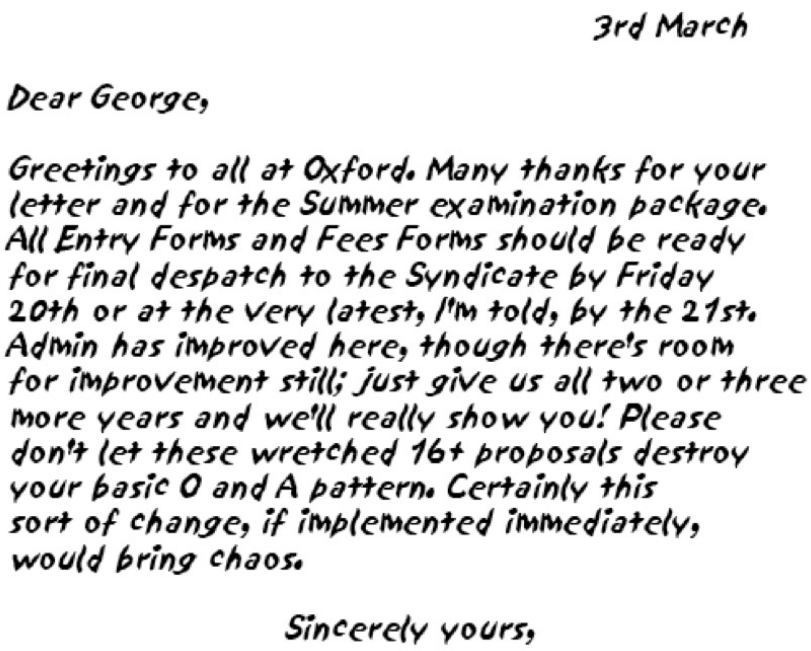

Figure 5.2. A puzzle for Inspector Morse.

2. Another technique for sending a hidden message is to send the message to everyone (and hence no one in particular), but in such a form that everyone but the intended recipient ignores it. David McKellar created a grammar that encodes messages in Spam-like phrases removed from his collection of Spam messages. You can see it in action at http://www.spammimic.com. If you are interested in learning more, check out Peter Wayner's wonderful book: "Disappearing Cryptography."

   The CS310-Fall16 course conference has been spammed. The messages reads

```
Dear Friend , This letter was specially selected to
be sent to you . This is a one time mailing there is
no need to request removal if you won't want any more
! This mail is being sent in compliance with Senate
```

```
bill 1618 ; Title 6 ; Section 304 ! This is NOT unsolicited
bulk mail . Why work for somebody else when you can
become rich in 38 days ! Have you ever noticed society
seems to be moving faster and faster and more people
than ever are surfing the web ! Well, now is your chance
to capitalize on this ! WE will help YOU use credit
cards on your website and turn your business into an
E-BUSINESS . You can begin at absolutely no cost to
you ! But don't believe us . Mr Jones of Indiana tried
us and says "I was skeptical but it worked for me"
! We assure you that we operate within all applicable
laws ! We IMPLORE you - act now ! Sign up a friend
and you get half off ! Best regards ! Dear Friend ,
We know you are interested in receiving cutting-edge
info ! This is a one time mailing there is no need
to request removal if you won't want any more . This
mail is being sent in compliance with Senate bill 1622
, Title 9 , Section 304 ! THIS IS NOT MULTI-LEVEL MARKETING
! Why work for somebody else when you can become rich
as few as 55 months ! Have you ever noticed people
will do almost anything to avoid mailing their bills
& people love convenience . Well, now is your chance
to capitalize on this . We will help you turn your
business into an E-BUSINESS & deliver goods right to
the customer's doorstep ! You are guaranteed to succeed
because we take all the risk . But don't believe us
! Prof Ames who resides in North Dakota tried us and
says "Now I'm rich many more things are possible" .
We assure you that we operate within all applicable
laws ! We beseech you - act now ! Sign up a friend
and you'll get a discount of 20% ! Cheers .
```

What does it really say? Notice anything special about the plaintext?