Exercise Sheet 1

Prof. Kenny Paterson, F. Günther
M. Backendal, M. Filić

Group Discussion (Basics). Take some time to think about and discuss:

(a) What, for you, is the most important application of cryptography?

(b) What's the difference between *cryptographic design* and *cryptanalysis*?

Suggested focus. Attempt these problems
before class: Problems 1, 2 and 3.
in class: Problem 4.
in your own time: Problems 5 and 6.

Suggested reading. Reading the following sections in the Boneh-Shoup book [1] might help with the problems on this exercise sheet: Sections 2.1, 2.2.1-2.2.3, 3.1, 3.2, and 3.3 (One-time pad, introduction to security games and reductions). Sections 4.1.1-4.1.2 (Block ciphers).

Problem 1 (Malleability of the One-time Pad). You just sat through the worst exam of your life and are heading home to start cramming for the next one, which is already tomorrow. Life feels hopeless and you start taking your frustration out on the world. In a moment of over-confidence, you decide to send your professor an angry email. You start typing "`Dear Professor, I hated your class so much. It sucked! Sincerely...`", but just before you hit send you get cold feet and decide to encrypt the message. You quickly choose a random key, *s bxbpy pbtz scomu dn qmhy af hxvysz*, encrypt the controversial parts of your message and hit send. The email reads: "`Dear Professor, a ixutb npnq unoem vb cgjf. iy zrxiwc! Hint: The message is encrypted with a one-time pad. Sincerely...`".

Next morning when you wake up, full of regrets, you have a message in your inbox from the professor asking you to come to their office and explain yourself. What will you do?! Devise a strategy to prove to the professor that your message was completely innocent.

Problem 2 (One-time Pad Cryptanalysis). You have intercepted two ciphertexts c and c'. You know that both are OTP ciphertexts encrypted with the *same* key k. For some fixed bit-strings m_0, m_0', m_1, m_1' you know that **either** c is an encryption of m_0 and c' is an encryption of m_0' **or** c is an encryption of m_1 and c' is an encryption of m_1'.

(a) Explain how to determine which of the two possibilities is true. Does it work in all cases?

(b) Now let $m_0 =$ "a", $m_0' =$ "b", $m_1 =$ "c", and $m_1' =$ "d" (all converted to binary from ASCII in the standard way). Let $c = 11111001$ and $c' = 11111010$.

Which of the two possibilities is correct? What was the key k?

Problem 3 (One-time Pad with Inconvenient Message and Key Spaces). Suppose you want to encrypt a single message $m \in \{0, 1, 2\}$ using a uniformly random shared key $k \in \{0, 1, 2\}$. Suppose you do this by representing each of k and m using two bits (00, 01, or 10), and then XOR-ing the two representations. Does this seem like a good algorithm to you? Explain. If not, then explain a better way to do this.

Problem 4 (Block Ciphers). Recall that a function $\mathsf{E}\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is called a *block cipher* if for all $\mathsf{K} \in \{0,1\}^k$, E_K is an efficiently computable permutation on $\{0,1\}^n$. Here $\mathsf{E}_\mathsf{K}(x) := \mathsf{E}(\mathsf{K}, x)$.

Let $\mathsf{E} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher.

(a) Let the function $\mathsf{F}_1 : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be defined by

$$\mathsf{F}_1(\mathsf{K}, x) = \mathsf{E}(\mathsf{K}, x) \oplus x.$$

Give an example illustrating that F_1 is not in general a block cipher.

Recall the definition of PRP security of a block cipher E, in which an adversary $\mathcal{A}$ with access to an oracle $\textsc{Fn}$ is asked to distinguish a "real world" ($b = 0$) where $\textsc{Fn}(x)$ returns the evaluation $\mathsf{E}(\mathsf{K}, x)$ under a random key K from a "random world" ($b = 1$) where $\textsc{Fn}(x)$ returns the evaluation $\Pi(x)$ under a randomly sampled permutation $\Pi\colon \{0,1\}^n \to \{0,1\}^n$. The advantage of $\mathcal{A}$ in this game is defined as $\mathbf{Adv}^{\mathrm{PRP}}_{\mathsf{E}}(\mathcal{A}) = 2 \cdot \left|\Pr\left[\,\text{Game } \mathbf{PRP}(\mathcal{A}, \mathsf{E}) \Rightarrow \mathsf{true}\,\right] - \frac{1}{2}\right|$, where $\Pr\left[\,\text{Game } \mathbf{PRP}(\mathcal{A}, \mathsf{E}) \Rightarrow \mathsf{true}\,\right]$ denotes the probability that the output of Game **PRP** is true.

Game $\mathbf{PRP}(\mathcal{A}, \mathsf{E})$:	Oracle $\textsc{Fn}(x)$:
1 $b \leftarrow\!\!\$\ \{0,1\}$	6 If $b = 0$ then:
2 $\mathsf{K} \leftarrow\!\!\$\ \{0,1\}^k$	7 $\quad y \leftarrow \mathsf{E}_\mathsf{K}(x)$
3 $\Pi \leftarrow\!\!\$\ \mathsf{Perms}[\{0,1\}^n]$	8 Else if $b = 1$ then:
4 $b' \leftarrow\!\!\$\ \mathcal{A}^{\textsc{Fn}}()$	9 $\quad y \leftarrow \Pi(x)$
5 Return $b' = b$	10 Return y

(b) Let the function $\mathsf{F}_2 : (\{0,1\}^k \times \{0,1\}^n) \times \{0,1\}^n \to \{0,1\}^n$ be defined by

$$\mathsf{F}_2((\mathsf{K}_1, \mathsf{K}_2), x) = \mathsf{E}(\mathsf{K}_1, \mathsf{K}_2 \oplus x).$$

The keyspace of F_2 is $\{0,1\}^k \times \{0,1\}^n$.

1) Show that F_2 is a block cipher.
2) Argue informally that F_2 is a pseudorandom permutation (i.e., is PRP-secure) assuming that E is a pseudorandom permutation.

We now want to formally prove that F_2 is PRP-secure assuming that E is PRP-secure.

For proving relations like this, we use a *reductionist* proof approach (conceptually following complexity-theoretic reductions). We start by taking the contra-position of the claim

$$\mathsf{E} \text{ PRP-secure} \implies \mathsf{F}_2 \text{ PRP-secure},$$

to arrive at the equivalent

$$\mathsf{F}_2 \underline{\text{ not}} \text{ PRP-secure} \implies \mathsf{E} \underline{\text{ not}} \text{ PRP-secure}.$$

The result is the reduction we want to construct: Assume F_2 is not PRP-secure, i.e., there exists an adversary $\mathcal{A}$ with high advantage against the PRP security of F_2. Then we construct a reduction algorithm $\mathcal{B}$ with high advantage against the PRP security of E (i.e., show that E is not PRP-secure).

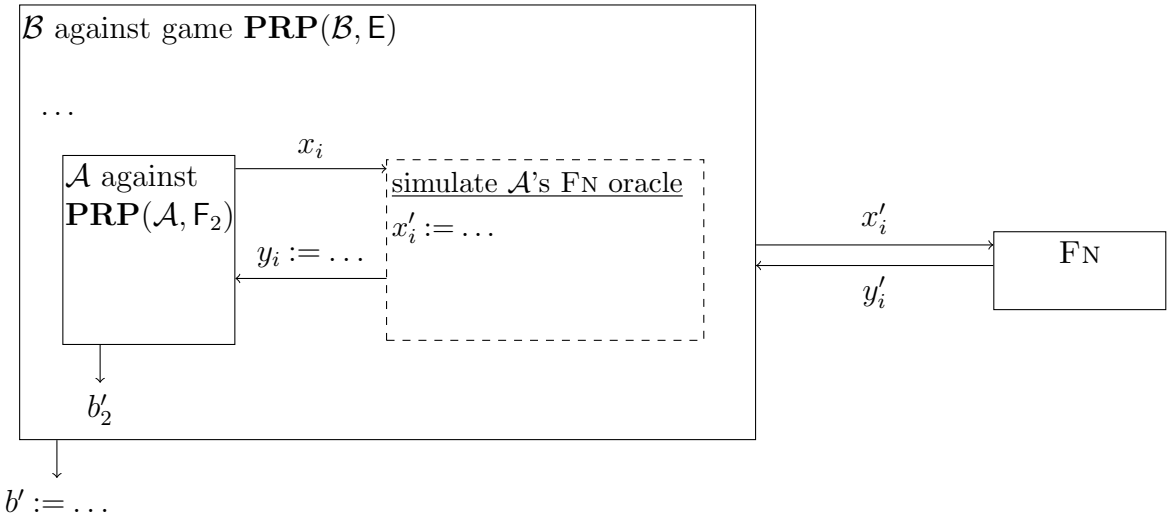
The idea for the reduction $\mathcal{B}$ is *simulate* the game $\mathbf{PRP}(\mathcal{A}, \mathsf{F}_2)$ for $\mathcal{A}$ by using the oracle $\mathcal{B}$ has available in its game $\mathbf{PRP}(\mathcal{B}, \mathsf{E})$. This should be done in such a way that, when $\mathcal{B}$'s oracle gives real (resp. random) responses, the simulated response to $\mathcal{A}$ should likewise be real (resp. random). We call such a simulation *sound*, if for $\mathcal{A}$ there's no observable difference between interacting with the game $\mathbf{PRP}(\mathcal{A}, \mathsf{F}_2)$ it expects and $\mathcal{B}$'s simulation. As a result, $\mathcal{B}$ can use $\mathcal{A}$'s bit guess to solve its own PRP security challenge.

Building the reduction $\mathcal{B}$ involves four steps:

1) Identify what $\mathcal{B}$ needs to do. We begin by comparing the games $\mathbf{PRP}(\mathcal{B}, \mathsf{E})$ and $\mathbf{PRP}(\mathcal{A}, \mathsf{F}_2)$ to determine what $\mathcal{B}$ needs to do/simulate "on top of" what $\mathbf{PRP}(\mathcal{B}, \mathsf{E})$ does already. To determine this, compare $\mathbf{PRP}(\mathcal{A}, \mathsf{F}_2)$ below with $\mathbf{PRP}(\mathcal{B}, \mathsf{E})$ and highlight those steps which are different/extra:

Game $\mathbf{PRP}(\mathcal{A}, \mathsf{F}_2)$:	Oracle $\textsc{Fn}(x)$:
1 $b \leftarrow\$ \{0,1\}$	6 If $b = 0$ then:
2 $\mathsf{K}_1 \leftarrow\$ \{0,1\}^k$; $\mathsf{K}_2 \leftarrow\$ \{0,1\}^n$	7 $\quad y \leftarrow \mathsf{F}_2((\mathsf{K}_1, \mathsf{K}_2), x) = \mathsf{E}(\mathsf{K}_1, \mathsf{K}_2 \oplus x)$
3 $\Pi \leftarrow\$ \mathsf{Perms}[\{0,1\}^n]$	8 Else if $b = 1$ then:
4 $b' \leftarrow\$ \mathcal{A}^{\textsc{Fn}}()$	9 $\quad y \leftarrow \Pi(x)$
5 Return $b' = b$	10 Return y

2) Define reduction $\mathcal{B}$. This can be done in words, pictorially, or in pseudocode. You may start with the pictorial representation below, similar to those used in the lecture, and fill in the "..." gaps. Then complete the pseudocode for $\mathcal{B}$. Make sure you can explain all this in words to a peer student.



Reduction $\mathcal{B}^{\text{FN}}$:	Oracle $\mathsf{FnSim}(x_i)$:
1 ...	4 $x'_i := \ldots$
2 $b'_2 \leftarrow\!\!\$\ \mathcal{A}^{\mathsf{FnSim}}()$	5 $y'_i \leftarrow \text{FN}(x'_i)$
3 Return ...	6 $y_i := \ldots$
	7 Return y_i

3) Argue why $\mathcal{B}$'s simulation for $\mathcal{A}$ is sound. That is, argue that when $\mathcal{B}$ gets real responses ($b = 0$ in $\mathbf{PRP}(\mathcal{B}, \mathsf{E})$), it correctly simulates real responses for $\mathcal{A}$, and vice versa for the random world ($b = 1$). Also say why $\mathcal{B}$ is efficient.

4) Translate the reduction into an advantage bound. Finally, argue that due to the above, $\mathcal{A}$'s advantage in breaking PRP security of F_2 is bounded by $\mathcal{B}$'s advantage in breaking PRP security of E.

(c) Let the function $\mathsf{F}_3 : (\{0,1\}^k \times \{0,1\}^n) \times \{0,1\}^n \to \{0,1\}^n$ be defined by

$$\mathsf{F}_3((\mathsf{K}_1, \mathsf{K}_2), x) = \mathsf{E}(\mathsf{K}_1, \mathsf{K}_2) \oplus x.$$

1) Show that F_3 is a block cipher.

2) Argue informally why F_3 is *not* a secure PRP.

3) To make the latter argument formal, define an adversary $\mathcal{A}$ attacking the PRP security of F_3.

Hint: There is an adversary $\mathcal{A}$ that makes exactly two *distinct* queries to its challenger (we call this a 2-query adversary) and achieves $\mathbf{Adv}^{\text{PRP}}_{\mathsf{F}_3}(\mathcal{A}) = 1 - \frac{1}{2^n - 1}$. (This almost-perfect distinguishing advantage is essentially the highest possible achievable advantage.)

Note that despite the similarities between F_2 and F_3, one is secure while the other is not. Think about how misplaced parentheses can have important consequences for security!

Problem 5 (Bonus: Historic Ciphers). Kerckhoff's principle essentially states that a cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

(a) Recover the English phrase that is encoded below using the Caesar cipher:

```
BPM MVMUG SVWEA BPM AGABMU
```

(b) The following explains the origin of the above phrase:

```
OXYGDOSYMW IYMGJMISI TZ JHYQNSEMLH UF GEHYWL WAHRGVR
```

Decrypt it using the Vigenère cipher with the key `ETH`.

Problem 6 (Challenge: Encryption with a Deck of Cards). Alice, Bob, and Eve are playing a card game. Alice shuffles a deck of cards and deals it all out to herself and Bob (each gets half of the 52 distinct cards). Alice now wishes to send a secret message m to Bob by saying something aloud. Everybody is in the same room, and eavesdropper Eve is listening in: she hears everything Alice says (but Eve cannot see the face of Alice's and Bob's cards).

(a) Suppose Alice's message m is a string of 48 bits. Describe how Alice can communicate m to Bob in such a way that Eve will have *no* information about the value of m.
Hint: Alice and Bob are allowed to devise a public strategy together *before* the cards are dealt.

(b) Now suppose that Alice's message m is 49 bits. Show that there exists no protocol that allows Alice to communicate m to Bob in such a way that Eve will have no information about m.

Acknowledgements. This exercise sheet is in part inspired by (and adapted from) problems by Rafael Pass, Tom Ristenpart, Mihir Bellare, Phillip Rogaway and Mark Zhandry, as well as from the book "A Graduate Course in Applied Cryptography" by Dan Boneh and Victor Shoup.

References

[1] D. Boneh and V. Shoup. *A Graduate Course in Applied Cryptography.* Online, version 0.6 edition, Jan. 2023.