Homework 1
CIS 5371: Cryptography

David Miller & Hannah McLaughlin
January 25, 2018

Problem 1: *In class, we learned about the dating problem and the 5-card trick. Prove that the trick protects the privacy of Bob.*

Let a message m in our message space $\mathcal{M}$ be a two-tuple {Alice's decision, Bob's decision} where 1 represents "yes" and 0 represents "no". To protect Bob's privacy we must show

$$\Pr_{K \xleftarrow{\$} \mathcal{K}} [\mathcal{E}_K(m_0) = c] = \Pr_{K \xleftarrow{\$} \mathcal{K}} [\mathcal{E}_K(m_1) = c] \tag{1}$$

where $m_0 = \{0, 1\}$, $m_1 = \{0, 0\}$, and c is some ciphertext. This can be shown via the group table for cuts made by Alice and Bob. This is because a cut in the deck is simply a shift. If we let p be the position where a cut is made then a cut maps $\text{Card}_i \to \text{Card}_{i-p \bmod 5}$ for $i = 0, ..., 4$. In fact the cut operation can be composed with another cut allowing us to represent the result from Alice's and Bob's cut in a group table. Letting $c_0(m_0)$ and $c_0(m_1)$ be the original ordering of cards before cuts, we can find the result after the two cuts with figure 1 where c_n represents the shift $\text{Card}_i \to \text{Card}_{i-p \bmod 5}$. The result after applying c_n is the ciphertext c.

Bob's Cut (columns); Alice's Cut (rows)

$\cdot$	c_0	c_1	c_2	c_3	c_4
c_0	c_0	c_1	c_2	c_3	c_4
c_1	c_1	c_2	c_3	c_4	c_0
c_2	c_2	c_3	c_4	c_0	c_1
c_3	c_3	c_4	c_0	c_1	c_2
c_4	c_4	c_0	c_1	c_2	c_3

$c_0(m_0)$:	♥♣♥♥♣	$c_0(m_1)$:	♥♣♥♣♥
$c_1(m_0)$:	♣♥♣♥♥	$c_1(m_1)$:	♥♥♣♥♣
$c_2(m_0)$:	♥♣♥♣♥	$c_2(m_1)$:	♣♥♥♣♥
$c_3(m_0)$:	♥♥♣♥♣	$c_3(m_1)$:	♥♣♥♥♣
$c_4(m_0)$:	♣♥♥♣♥	$c_4(m_1)$:	♣♥♣♥♥

Figure 1: Group table of shifts on m_0 and m_1 and their corresponding outcome.

Since we are considering Alice's viewpoint, we have a prescribed cut c_m by Alice. Now Bob randomly picks c_n for n uniformly distributed over $0, \ldots, 4$. The composition $c_{m+n \, mod \, 5}$ will be a secret cyclic shift to Alice via $\text{Card}_i \to \text{Card}_{i-p \bmod 5}$. Since $c_0(m_1) = c_2(m_0)$ we get

$$\Pr_{K \xleftarrow{\$} \mathcal{K}} [\mathcal{E}_K(m_0) = c] = \frac{1}{5} = \Pr_{K \xleftarrow{\$} \mathcal{K}} [\mathcal{E}_K(m_1) = c] \tag{2}$$

from Alice's perspective and therefore the privacy of Bob is protected. $\square$

Problem 2: *Alice shuffles a deck of cards and deals it out to herself and Bob so that each gets half of the 52 cards. Alice now wishes to send a secret message M to Bob by saying something aloud. Eavesdropper Eve is listening in hearing everything Alice says but cant see the cards.*

Part A: *Suppose Alice's message M is a string of 48-bits, so the message space M = {0, 1}^{48}. Describe how Alice can communicate M to Bob to achieve perfect secrecy.*

Let $\mathcal{M}$ denote the message space of 48-bit strings, and $\mathcal{C}$ denote the ciphertext space. We have that $|\mathcal{M}| = 2^{48} < {}_{52}C_{26} = |\mathcal{K}|$ and therefore $|\mathcal{C}| = |\mathcal{K}|$. Now define the encryption algorithm as

$$\mathcal{E}_K(m) : \mathcal{M} \to \mathcal{C} \tag{3}$$
$$\mathcal{E}_K(m) = (m + k) \mod {}_{52}C_{26} \tag{4}$$

for $k \in \mathcal{K}, c \in \mathcal{C}$. Respectively, define the decryption algorithm as

$$\mathcal{E}_K^{-1}(c) : \mathcal{C} \to \mathcal{M} \tag{5}$$
$$\mathcal{E}_K^{-1}(c) = (c - k) \mod 2^{48} \tag{6}$$

for $k \in \mathcal{K}, c \in \mathcal{C}$. Both $\mathcal{E}_K, \mathcal{E}_K^{-1}$ are one-to-one functions and therefore deterministic. To prove perfect secrecy we must show (1). It will be shown from implication rather than directly. For $m \in \mathcal{M}, c \in \mathcal{C}$ we have

$$\Pr_{K \xleftarrow{\$} \mathcal{K}}[\text{Alice says } c \,|\, M = m] = \Pr_{K \xleftarrow{\$} \mathcal{K}}[\mathcal{E}_K(m) = c \ \text{mod}_{52}C_{26}] = \tag{7}$$

$$\Pr_{K \xleftarrow{\$} \mathcal{K}}[\mathcal{E}_K(m) = (m + (c - m)) \ \text{mod}_{52}C_{26}] = \Pr_{K \xleftarrow{\$} \mathcal{K}}[k = (c - m) \ \text{mod}_{52}C_{26}] = \frac{1}{{}_{52}C_{26}}. \tag{8}$$

It follows from (7) and (8) that

$$\Pr_{K \xleftarrow{\$} \mathcal{K}}[\mathcal{E}_K(m_0) = c] = \Pr_{K \xleftarrow{\$} \mathcal{K}}[\mathcal{E}_K(m_1) = c] \tag{9}$$

for $m_0, m_1 \in \mathcal{M}, c \in \mathcal{C}$. It is important to note for (7) and (8) we used the fact that the key is sampled from a uniform distribution. $\square$

Part B: *Now suppose Alice's message M is 49 bits, so the message space is M = {0, 1}^{49}. Prove that there exists no protocol that allows Alice to communicate M to Bob to achieve perfect secrecy.*

Let $\mathcal{M}$ denote the message space of 49-bit strings. Now we have $|\mathcal{K}| = {}_{52}C_{26} < 2^{49} = |\mathcal{M}|$ and therefore $|\mathcal{C}| = |\mathcal{K}|$.

Proof 1: Since $|\mathcal{K}| < |\mathcal{M}|$ there exists $m_0, m_1 \in \mathcal{M}$ such that $\mathcal{E}_k(m_0) = \mathcal{E}_k(m_1) = c$ for some ciphertext $c \in \mathcal{C}$. Therefore

$$\Pr_{K \xleftarrow{\$} \mathcal{K}} [\mathcal{E}_K(m_0) = c] = \Pr_{K \xleftarrow{\$} \mathcal{K}} [\mathcal{E}_K(m_0) = \mathcal{E}_K(m_1)] = \Pr_{K \xleftarrow{\$} \mathcal{K}} [\mathcal{E}_K(\mathcal{E}_K^{-1}(c)) = \mathcal{E}_K(m_1)] \tag{10}$$

$$\Pr_{K \xleftarrow{\$} \mathcal{K}} [\mathcal{E}_K(m_1) = \mathcal{E}_K(m_1)] = 1 \tag{11}$$

We have arrived at the contradiction

$$\Pr_{K \xleftarrow{\$} \mathcal{K}} [\mathcal{E}_K(m_0) = c] = 1 \tag{12}$$

since key K is sampled from a uniform distribution on $\mathcal{K}$ and $|\mathcal{K}| > 1$. $\square$

Proof 2: We shall prove $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{E}^{-1})$ with message space $\mathcal{M}$ and cipertext space $\mathcal{C}$ needs the property $|\mathcal{M}| \leq |\mathcal{K}|$ to be perfectly secure.

Suppose $|\mathcal{K}| < |\mathcal{M}|$. Let $\mathcal{E}_{K'}(m') = c'$ for some $K' \in \mathcal{K}, m' \in \mathcal{M}, c' \in \mathcal{C}$. It follows that

$$\Pr_{K \xleftarrow{\$} \mathcal{K}} [\mathcal{E}_K(m') = c'] > 0 \tag{13}$$

Let $Q = \{\mathcal{E}_K^{-1}(c') \,|\, K \in \mathcal{K})\}$, which is just deciphering c' with all possible keys. Since $|Q| \leq |\mathcal{K}| < |\mathcal{M}|$ we have $|\mathcal{Q}| < |\mathcal{M}|$ by transitivity. Therefore there exists a $m^* \in \mathcal{M}$ such that $m^* \notin Q$. Now trying to encrypt m^* with all possible keys we get

$$\mathcal{E}_K(m^*) \neq c' \quad \Rightarrow \quad \Pr_{K \xleftarrow{\$} \mathcal{K}} [\mathcal{E}_K(m^*) = c'] = 0 \tag{14}$$

for all $K \in \mathcal{K}$. Therefore there exists $m', m^* \in \mathcal{M}$ and $c' \in \mathcal{C}$ such that

$$\Pr_{K \xleftarrow{\$} \mathcal{K}} [\mathcal{E}_K(m') = c'] \neq \Pr_{K \xleftarrow{\$} \mathcal{K}} [\mathcal{E}_K(m^*) = c'] \tag{15}$$

which contradicts perfect secrecy. Since our problem has the property $|\mathcal{K}| < |\mathcal{M}|$, Alice and Bob can not have a protocol that admits perfect secrecy. $\square$