Volume 2 (2021), Article 1 https://research.library.kutztown.edu/contact/

CONTACT
COMMUNICATIONS ON NUMBER THEORY
AND COMBINATORIAL THEORY

Determining Biases in the Card-Chameleon Cryptosystem

Isaac Reiter*[1] and Eric Landquist†[1]

[1]Department of Mathematics, Kutztown University of Pennsylvania

First submitted: July 13, 2020
Accepted: February 28, 2021
Published: March 8, 2021

Abstract

Throughout history, spies, soldiers, and others have relied on so-called *hand ciphers* to send encrypted messages. Since the creation of Pontifex (also known as Solitaire) by Bruce Schneier in 1999, a number of hand ciphers utilizing a standard deck of playing cards have emerged. Since there are $52! \approx 2^{225.58}$ possible ways to order a deck of cards, there are over 225 bits of entropy in a well-shuffled deck of cards. Theoretically, this can provide enough security to rival modern computer-based cryptosystems. In this paper, we describe and analyze one such playing card cipher, Card-Chameleon, created by Matthew McKague. Our analysis reveals new weaknesses in this cryptosystem, particularly the tendency for a letter to encrypt to itself. This bias makes it easy to recover the plaintext if it is encrypted into multiple different ciphertexts. We will describe variations of Card-Chameleon which significantly reduced these weaknesses but did not completely eliminate them.

Keywords: cryptanalysis, hand cipher, card cipher, playing cards, cryptography

*ireit426@live.kutztown.edu
†elandqui@kutztown.edu

1 Introduction

Throughout history, soldiers, spies, and others have relied on so-called *hand ciphers* or *field ciphers* to send brief encrypted information for tactical purposes. Before the mechanization of cryptography in the early 20th century, nearly all ciphers could be considered hand ciphers. However, historical cipher machines, such as ENIGMA, were impractical for many agents to use in the field, so hand ciphers were designed to use a minimal amount of equipment. Modern computerized ciphers and online transmission could also leave a digital trail leading to an agent, so hand ciphers are used when the sender and receiver want to avoid having an electronic footprint. Hand ciphers are also used as a back-up when standard encryption is impossible. In 1999, author Neal Stephenson commissioned security expert Bruce Schneier to develop a secure hand cipher using playing cards for his novel *Cryptonomicon* [6]. Schneier's cipher, *Solitaire*, code-named *Pontifex* in the novel, "is low-tech, but its security is designed to be high-tech." [4]

There are a myriad of reasons for using playing cards in order to encrypt information. First, playing cards are convenient and inexpensive. Second, they are common enough so as not to arouse suspicion if a deck is found in an agent's possession. Third, since there are 52 cards in a standard deck, the cards perfectly encode all uppercase and lowercase English letters. Finally, and most importantly, there are $52! \approx 2^{225.58}$ possible permutations of a deck of cards, providing over 225 bits of entropy. By comparison, industrial-grade encryption using AES, for example, uses 128 to 256 bits of entropy to create a secret encryption key. Thus, a well-shuffled deck of playing cards possesses a level of entropy allowing for a cryptosystem based on this deck to have a level of security to rival modern ciphers like AES.

With this motivation and inspiration from Schneier's Solitaire, a number of researchers have created other playing-card based ciphers. Many have also analyzed Solitaire and other playing card ciphers. For the interested reader, descriptions and analysis of a number of playing card ciphers can be found at the website of Aaron Toponce, a system administrator [7]. One such playing card cipher is called Card-Chameleon and was developed by Matthew McKague as part of his master's thesis at the University of Waterloo under the direction of well-known cryptographer Alfred Menezes [2]. McKague drew inspiration for Card-Chameleon from Solitaire and the stream cipher RC4 developed by Ron Rivest [3]. McKague's thesis describes a playing card version of RC4 as well.

In this paper, we will describe Card-Chameleon and note some of the attacks that have been made on the cipher. We will then describe new attacks on Card-Chameleon. If Card-Chameleon is used to encrypt the same message with multiple different keys, then it is possible to reconstruct the original message. We then describe and analyze modifications to Card-Chameleon to reduce the weaknesses in the original cipher. This paper contains the first cryptanalysis of Card-Chameleon outside of McKague's thesis.

2 Definitions and Notation

Throughout this paper, we will use various examples of deck orders. We will use brackets to represent a deck order. As the cards are listed from left to right, these denote the cards from bottom to top. For example, $[A\spadesuit, \ldots, A\heartsuit]$ represents a deck order in which $A\spadesuit$ is on the bottom and $A\heartsuit$ is on the top. A subset of the deck will be represented by braces, for example, $\{5\diamondsuit, J\clubsuit\}$ to represent the two-card sequence with $J\clubsuit$ above $5\diamondsuit$. We will represent a joker with $\mathcal{J}$.

Definition 2.1. When a red card immediately follows a black card, we will refer to these cards as **paired**.

Definition 2.2. When a card represents the same letter as another card, we will refer to these cards as **congruent** to each other. Also, a **congruent pair** is a black card and a red card that represent the same letter.

Definition 2.3. When two consecutive letters are the same (e.g. `AA`), we will refer to this as a **double**. If the letters are different (e.g. `AB`), we will call this a **non-double**.

3 Description of Card-Chameleon

To determine the encryption and decryption key, the deck is thoroughly shuffled and arranged face-up, alternating red and black cards, with a red card on top. This deck order is the encryption and decryption key, so the sender and receiver must have the same ordering of the deck in their possession. Because of this setup, there are $(26!)^2 \approx 2^{176.76}$ possible keyed decks. Thus, Card-Chameleon takes advantage of over 176 bits of entropy.

Each card encodes a letter, as shown in Table 1; each letter is represented by one black card and one red card. This encryption scheme is not case-sensitive, so there is no distinction between uppercase and lowercase letters. For consistency, we will use uppercase letters.

	Spades and Hearts ($\spadesuit, \heartsuit$)												
Card	A	2	3	4	5	6	7	8	9	10	J	Q	K
Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
	Clubs and Diamonds ($\clubsuit, \diamondsuit$)												
Card	A	2	3	4	5	6	7	8	9	10	J	Q	K
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Table 1: Letter encoding for Card-Chameleon

3.1 Initialization Vectors

As we will see, the position of the black cards in a deck will not change relative to each other when encrypting a message. This alone presents a means to attack Card-Chameleon if a key is used twice. Therefore, it is advisable to use an **initialization vector** (IV) of 26 letters to permute a deck before encrypting a message. The IV is sent to the receiver as the first 26 letters of the ciphertext. The following steps permute the deck with an IV. For each letter of the IV, do the following.

1. Using Table 1, find the black card that represents the IV letter.

2. Look at the red card above this black card. Call this red card ρ, the card *paired* with the black card.

3. Card ρ represents the same letter as another black card. Locate the black card, card β, in the deck *congruent* to ρ.

4. Switch the red card above β with the top card.

5. Move β and the red card above β to the bottom of the deck.

6. Move the top two cards to the bottom of the deck.

Note that these steps can also be used in lieu of shuffling to key the deck with a string of letters starting from an agreed default order that alternates black and red cards, such as $[K\clubsuit, K\diamondsuit, Q\clubsuit, Q\diamondsuit, \ldots, 2\spadesuit, 2\heartsuit, A\spadesuit, A\heartsuit]$. A random letter has $\log_2(26) \approx 4.7$ bits of entropy, so 38 random letters is a sufficiently long keystring to key the deck with the maximum possible entropy.

3.2 Encryption

Card-Chameleon is a stream cipher, encrypting a message one letter at a time with a six-step algorithm similar to IV procedure above.

1. Find the black card that represents the plaintext letter.

2. Look at the paired red card above this black card.

3. Locate the congruent black card in the deck.

4. The paired red card above this black card represents the ciphertext letter.

5. Switch the red ciphertext card with the red card that is on the top of the deck. If the ciphertext card is already on top of the deck, this step can be skipped.

6. Move the top two cards to the bottom of the deck.

To demonstrate this process, we will encrypt `ATTACK AT DAWN` with Card-Chameleon using the following keyed deck.

$$\begin{gathered}[7\spadesuit, 3\diamondsuit, 6\spadesuit, K\heartsuit, 4\clubsuit, A\heartsuit, A\clubsuit, 3\heartsuit, 3\spadesuit, 10\diamondsuit, 10\clubsuit, Q\diamondsuit, 6\clubsuit,\\ A\diamondsuit, 9\clubsuit, 8\heartsuit, Q\spadesuit, 4\heartsuit, K\spadesuit, J\heartsuit, 3\clubsuit, 8\diamondsuit, Q\clubsuit, 7\heartsuit, A\spadesuit, 10\heartsuit,\\ J\spadesuit, 2\diamondsuit, 2\clubsuit, Q\heartsuit, 4\spadesuit, K\diamondsuit, 7\clubsuit, 9\heartsuit, 8\clubsuit, 5\heartsuit, 5\spadesuit, 6\heartsuit, 9\spadesuit,\\ 6\diamondsuit, 2\spadesuit, 9\diamondsuit, 10\spadesuit, 7\diamondsuit, J\clubsuit, 2\heartsuit, 5\clubsuit, 4\diamondsuit, K\clubsuit, 5\diamondsuit, 8\spadesuit, J\diamondsuit]\end{gathered}$$

In order to encrypt the first `A`, Table 1 tells us to first find $A\spadesuit$. Second, we notice that above (i.e., after) $A\spadesuit$ is $10\heartsuit$. Third, $10\heartsuit$ and $10\spadesuit$ are a congruent pair. Thus, we now find $10\spadesuit$. Fourth, the card that is above $10\spadesuit$ is $7\diamondsuit$, which represents `T`. Thus, `A` encrypts to

`T`. Now we rearrange the deck. We switch $7\diamondsuit$ with the top (right-most) card, which is $J\diamondsuit$. Then we move the top two cards, $8\spadesuit$ and $7\diamondsuit$, to the bottom of the deck. Now the order of the deck is as follows.

$$\begin{gathered}[8\spadesuit, 7\diamondsuit, 7\spadesuit, 3\diamondsuit, 6\spadesuit, K\heartsuit, 4\clubsuit, A\heartsuit, A\clubsuit, 3\heartsuit, 3\spadesuit, 10\diamondsuit, 10\clubsuit,\\ Q\diamondsuit, 6\clubsuit, A\diamondsuit, 9\clubsuit, 8\heartsuit, Q\spadesuit, 4\heartsuit, K\spadesuit, J\heartsuit, 3\clubsuit, 8\diamondsuit, Q\clubsuit, 7\heartsuit,\\ A\spadesuit, 10\heartsuit, J\spadesuit, 2\diamondsuit, 2\clubsuit, Q\heartsuit, 4\spadesuit, K\diamondsuit, 7\clubsuit, 9\heartsuit, 8\clubsuit, 5\heartsuit, 5\spadesuit,\\ 6\heartsuit, 9\spadesuit, 6\diamondsuit, 2\spadesuit, 9\diamondsuit, 10\spadesuit, J\diamondsuit, J\clubsuit, 2\heartsuit, 5\clubsuit, 4\diamondsuit, K\clubsuit, 5\diamondsuit]\end{gathered}$$

Next, we encrypt the letter `T`. First, we find $7\clubsuit$. Second, $9\heartsuit$ is above $7\clubsuit$. Third, since $9\heartsuit$ and $9\spadesuit$ are a congruent pair, we find $9\spadesuit$. Fourth, $6\diamondsuit$ is above $9\spadesuit$. Thus, the letter `T` encrypts to `S`. Again, we rearrange the deck. We switch $6\diamondsuit$ with the top card, which is $5\diamondsuit$. Then we move the top two cards, $K\clubsuit$ and $6\diamondsuit$, to the bottom. This gives us the following deck order.

$$\begin{gathered}[K\clubsuit, 6\diamondsuit, 8\spadesuit, 7\diamondsuit, 7\spadesuit, 3\diamondsuit, 6\spadesuit, K\heartsuit, 4\clubsuit, A\heartsuit, A\clubsuit, 3\heartsuit, 3\spadesuit,\\ 10\diamondsuit, 10\clubsuit, Q\diamondsuit, 6\clubsuit, A\diamondsuit, 9\clubsuit, 8\heartsuit, Q\spadesuit, 4\heartsuit, K\spadesuit, J\heartsuit, 3\clubsuit, 8\diamondsuit,\\ Q\clubsuit, 7\heartsuit, A\spadesuit, 10\heartsuit, J\spadesuit, 2\diamondsuit, 2\clubsuit, Q\heartsuit, 4\spadesuit, K\diamondsuit, 7\clubsuit, 9\heartsuit, 8\clubsuit,\\ 5\heartsuit, 5\spadesuit, 6\heartsuit, 9\spadesuit, 5\diamondsuit, 2\spadesuit, 9\diamondsuit, 10\spadesuit, J\diamondsuit, J\clubsuit, 2\heartsuit, 5\clubsuit, 4\diamondsuit]\end{gathered}$$

After repeating these steps for the rest of the message, we get the ciphertext: `TSRXYL YY SQLW`.

3.3 Decryption

The process to decrypt a ciphertext is a straightforward reversal of the encryption steps.

1. Find the red card that represents the ciphertext letter.
2. Look at the black card below this red card.
3. Locate the congruent card in the deck.
4. The black card below this red card represents the plaintext letter.
5. Switch the red card in step 1 with the top red card. If it is already on the top of the deck, this step can be skipped.
6. Move the top two cards to the bottom of the deck.

In order to decrypt `TSRXYL YY SQLW` with the following keyed deck order, we will start with `T`.

$$\begin{gathered}[7\spadesuit, 3\diamondsuit, 6\spadesuit, K\heartsuit, 4\clubsuit, A\heartsuit, A\clubsuit, 3\heartsuit, 3\spadesuit, 10\diamondsuit, 10\clubsuit, Q\diamondsuit, 6\clubsuit,\\ A\diamondsuit, 9\clubsuit, 8\heartsuit, Q\spadesuit, 4\heartsuit, K\spadesuit, J\heartsuit, 3\clubsuit, 8\diamondsuit, Q\clubsuit, 7\heartsuit, A\spadesuit, 10\heartsuit,\\ J\spadesuit, 2\diamondsuit, 2\clubsuit, Q\heartsuit, 4\spadesuit, K\diamondsuit, 7\clubsuit, 9\heartsuit, 8\clubsuit, 5\heartsuit, 5\spadesuit, 6\heartsuit, 9\spadesuit,\\ 6\diamondsuit, 2\spadesuit, 9\diamondsuit, 10\spadesuit, 7\diamondsuit, J\clubsuit, 2\heartsuit, 5\clubsuit, 4\diamondsuit, K\clubsuit, 5\diamondsuit, 8\spadesuit, J\diamondsuit]\end{gathered}$$

First, we find the red card that represents the `T`, which is $7\diamondsuit$. Second, the card below $7\diamondsuit$ is $10\spadesuit$. Third, we find $10\heartsuit$ in the deck. Fourth, the card below $10\heartsuit$ is $A\spadesuit$. Thus, the letter `T` decrypts to `A`. Then we switch the deck order. $7\diamondsuit$ is switched with the top card, $J\diamondsuit$. Sixth, the top two cards $8\spadesuit$ and $7\diamondsuit$, are moved to the bottom. We then continue to decrypt the rest of the letters, allowing us to read `ATTACK AT DAWN`.

3.4 Known Attacks

With over 176 bits of entropy, a brute-force attack on Card-Chameleon is infeasible. An unpublished claim of a chosen plaintext attack with 96 bits of complexity was posted on GitHub [5]. The branch-and-bound attack of Knudsen et al. on RC4 can be modified to Card-Chameleon with a complexity of 88 bits [**?**, 2], which is still infeasible. This was previously the best known attack. Our attacks will also show the need for an IV if one encrypts the same message to multiple parties.

4 Biases in Card-Chameleon: Individual Letters

The following results outline the main new attack on Card-Chameleon. With a perfect encryption scheme, like the One-Time Pad (OTP), a letter will encrypt to itself with probability $\frac{1}{26}$. However, we have the following.

Theorem 4.1. *Assuming that the deck is in a random order for each letter, the probability that a letter in the plaintext will encrypt to itself is* $\frac{1}{13}$.

Proof. Without loss of generality, suppose we are encrypting the letter `A`. There are two types of keyed decks that will encrypt `A` to itself. If `A` encrypts to `A`, then in the encryption process, we first find the black card corresponding with `A`: $A\spadesuit$. Let R be the red card above $A\spadesuit$. Next, we find, B, the black card that is congruent to R. Finally, we must have $A\heartsuit$ above B, yielding the ciphertext letter `A`. Therefore, the deck contains the sequence $\{A\spadesuit, R, \ldots, B, A\heartsuit\}$ or $\{B, A\heartsuit, \ldots, A\spadesuit, R\}$. So either $R = A\heartsuit$ and $B = A\spadesuit$ or R and B are one of the other 25 congruent pairs.

Case 1: $R = A\heartsuit$ and $B = A\spadesuit$, so $A\spadesuit$ and $A\heartsuit$ are paired with each other. After $A\heartsuit$ is placed above $A\spadesuit$, these two cards can be placed in 26 places in the deck. The rest of the deck can now be permuted in $(25!)^2$ ways. Thus, there are $26 \cdot (25!)^2$ keyed decks and the probability of Case 1 occurring is $\frac{26 \cdot (25!)^2}{(26!)^2} = \frac{1}{26}$.

Case 2: $R \neq A\heartsuit$ and $B \neq A\spadesuit$, so $A\heartsuit$ and $A\spadesuit$ are not paired with each other, but they are paired with two cards that form a congruent pair. $A\spadesuit$ and R can be placed in 26 places in the deck. Next, $A\heartsuit$ and B can be placed in 25 places in the deck. Third, $A\spadesuit$ and $A\heartsuit$ can be paired with one of 25 congruent pairs. Finally, the rest of the deck can be permuted in $(24!)^2$ ways. Thus, there are $26 \cdot 25 \cdot 25 \cdot (24!)^2 = 26 \cdot (25!)^2$ keyed decks, so the probability of Case 2 occurring is $\frac{26 \cdot (25!)^2}{(26!)^2} = \frac{1}{26}$.

Therefore, the probability of one of these decks occurring is $\frac{1}{26} + \frac{1}{26} = \frac{1}{13}$. □

This is a glaring statistical bias and therefore a significant weakness of this cryptosystem. However, an important caveat of this result is that it assumes that each letter is encrypted with a random deck. The following section demonstrates that the $\frac{1}{13}$ probability decreases when the same letter is encrypted more than once. This attack will be demonstrated empirically in Section 6.

5 Biases in Card-Chameleon: Double Letters

With a perfect encryption scheme, like the OTP, the probability that a double will encrypt to a double is $\frac{1}{26}$ and the probability that a double will encrypt to itself is $\frac{1}{676}$. The following result shows another weakness in which, in particular, it is four times more likely that Card-Chameleon will encrypt a double to itself.

Theorem 5.1. *Assuming that the deck is in a random order for each letter, the probability that a double in the plaintext will encrypt to:*

1. *itself is* $\frac{4}{26^2} = \frac{4}{676} = \frac{1}{169}$,
2. *a different double is* $\frac{24}{676} = \frac{6}{169}$, *and*
3. *any double is* $\frac{28}{676} = \frac{7}{169}$.

Proof. Without loss of generality, suppose that we are encrypting `AA`. There are five types of keyed decks that will encrypt a double to a double. We will first consider the keyed decks that encrypt `AA` to `AA`. As described in the proof of Theorem 4.1, there are two possibilities. Either $A\spadesuit$ and $A\heartsuit$ are paired, or they are not. If they are paired, then $A\spadesuit$ and $A\heartsuit$ can be on top of the deck or below the top. Cases 1 and 2 handles these two situations. If the two aces are not paired, then they must be paired with cards that form a congruent pair. Otherwise, the first `A` will not encrypt to `A`. Here again, we have two more scenarios. Either $A\spadesuit$ and its paired card are on top, or $A\heartsuit$ and its paired card are on top. If neither pair of cards is on top, the second `A` will not encrypt to `A`. These two scenarios are discussed in Cases 3 and 4. Finally, consider the keyed decks that will encrypt `AA` to a different double altogether. Here, we want to avoid $A\heartsuit$ in favor of a different red card R. Thus the deck is arranged as follows, with r and b representing a congruent pair: $[\ldots, A\spadesuit, r, \ldots, b, R]$ Notice that while $A\spadesuit$ and its paired card can be placed anywhere below the top, R must be on top. This is because it must stay above b in order for `A` to map to $A\spadesuit$, which maps to r, which maps to b, which maps to R. If R is not on top, it will be switched with the top card. This situation is handled by Case 5.

Case 1: $A\spadesuit$ and $A\heartsuit$ are paired, and they are on the top of the deck. Since the deck is ordered $[\ldots, A\spadesuit, A\heartsuit]$, when we encrypt `A`, we find $A\spadesuit$, then look above it to $A\heartsuit$. Since these two cards are a congruent pair, we go back to $A\spadesuit$ and subsequently $A\heartsuit$. Hence, `A` encrypts to `A`. Since the two aces are on top, they are simply moved to the bottom before we encrypt the next `A`. The same process will encrypt this second `A` to `A`. Thus, `AA` encrypts to `AA`. To count the possibilities of this, after $A\spadesuit$ and $A\heartsuit$ are placed on top, the rest of the deck can be permuted in $(25!)^2$ ways. Thus, there are $(25!)^2$ keyed decks, so the probability of Case 1 occurring is $\frac{(25!)^2}{(26!)^2} = \frac{1}{676}$.

Case 2: $A\spadesuit$ and $A\heartsuit$ are paired, they are not on top, and a congruent pair is on top. Since the two aces are together, the first `A` will encrypt to itself. After step five, notice that the card that is above $A\spadesuit$ and the card that is under $A\heartsuit$ are a congruent pair. Thus, the second `A` will also encrypt to itself. To count the possibilities of this, the $A\spadesuit$ and $A\heartsuit$ pair can be placed in 25 places in the deck. Next, 25 congruent pairs can be placed on top. Finally, the rest of the deck can be permuted in $(24!)^2$ ways. Thus, there are $25 \cdot 25 \cdot (24!)^2 = (25!)^2$ keyed decks and the probability of Case 2 occurring is $\frac{(25!)^2}{(26!)^2} = \frac{1}{676}$.

Case 3: $A\spadesuit$ is second from the top, $A\heartsuit$ is below the top, and the cards with which $A\spadesuit$ and $A\heartsuit$ are paired form a congruent pair. After the first `A` encrypts to itself, $A\heartsuit$ will switch places with the top card and be above $A\spadesuit$. Thus, the second `A` will also encrypt to itself. To count the possibilities, once $A\spadesuit$ is second from the top, $A\heartsuit$ can be placed in 25 places. Next, $A\spadesuit$ and $A\heartsuit$ can be paired with 25 congruent pairs. Finally, the rest of the deck can be permuted in $(24!)^2$ ways. Thus, there are $(25!)^2$ keyed decks and the probability of Case 3 occurring is $\frac{(25!)^2}{(26!)^2} = \frac{1}{676}$.

Case 4: $A\heartsuit$ is on top, $A\heartsuit$ is not paired with $A\spadesuit$, and the two aces are paired with a congruent pair. After the first `A` encrypts to itself, notice that since $A\heartsuit$ is on top, it will not be switched with a different card. Hence, the two aces will still be paired with a congruent pair, and the second `A` will encrypt to `A`. To count the possibilities, after $A\heartsuit$ is placed on top, $A\spadesuit$ can be put in 25 different locations. There are also 25 possible congruent pairs to pair with $A\spadesuit$ and $A\heartsuit$. The rest of the deck can be arranged in $(24!)^2$ possible ways. Thus, there are $25 \cdot 25 \cdot (24!)^2 = (25!)^2$ possible keyed decks, so the probability of Case 4 occurring is again $\frac{1}{676}$.

Cases 1-4 encrypt `AA` to `AA`, and there is a $\frac{4}{676} = \frac{1}{169}$ probability of that occurring. This establishes part (1).

Case 5: $A\spadesuit$ is below the second from the top, and the cards with which $A\spadesuit$ and the top card are paired form a congruent pair. The proof for this case is similar to the one for Case 4. To count the possibilities, $A\spadesuit$ can be placed in 25 places. Also, there are 25 possible top cards. Next, $A\spadesuit$ and the top card can be paired with 24 congruent pairs. Finally, the rest of the deck can be permuted in $(24!)^2$ ways. Thus, there are $25 \cdot 25 \cdot 24 \cdot (24!)^2 = 24 \cdot (25!)^2$ keyed decks, so the probability of Case 5 occurring is $\frac{24 \cdot (25!)^2}{(26!)^2} = \frac{24}{676}$. This establishes part (2).

The probability that a double will encrypt a double is therefore $\frac{28}{676}$, establishing part (3). □

6 A Practical Attack

To illustrate the bias of a letter encrypting to itself, we encrypted the same 34-letter sentence using $1040 = 40 \cdot 26$ pseudorandom keys. We used a `C++` program to generate these keys. For each key, two arrays (one for red cards and one for black cards) were initialized to `[0, 1, ..., 25]` and we used the `rand()` function modulo 26 and the Fisher-Yates shuffle [1] to generate the pseudorandom shuffle. If there were no bias, then for each $1 \leq i \leq 34$, we would expect each letter to appear 40 times in each set of ith letters among the 1040 ciphertexts. Theorem 4.1 suggests that the plaintext letter will appear 80 times. The following is a sample of the ciphertexts.

```
wkqouhvdxxraticeyljwpljegojckpkdyw
```

```
fffeyjxahulqlnkdudnlddidbtmgwouawi
mxbdgwgxiqspnoyuihztfoqoikflcraqyn
uydxzfgffcvpttneeqentqaeikfiyytslu
zhpevebboahwoaanyftoodibkvzxlghvkv
bbqdjumzgzxpngkmowjqfmrtchoabhxpwp
zagtdzkoextlujwddvreusbeinmiastuuy
lxpfuxnwyawgjrwnsqjylqovqkpbdeepno
qsgsanvhglbpzeflxnzgmaclkiiuoyzjul
```

If we take the most frequent letter in each column, we have the following.

```
thesundiwnotshineztwastokwefhcplay
```

This does not fully recover the plaintext, but we can determine enough of the plaintext to insert spaces and surmise the rest.

```
Spaces:  The sun diw not shine zt was tok wef hc play.
Actual:  The sun did not shine it was too wet to play.
```

One observation is that not every plaintext letter was the most frequent ciphertext letter. The instances in which the attack failed to find the actual plaintext letter were cases in which the plaintext letter appeared six letters or less before.

The following table shows the statistics on the frequency of the plaintext letter and most frequent letter in each column.

Plaintext	t 85	h 74	e 95	s 93	u 79	n 83	d 94	i 89	d 48	n 58	o 82	t 59	s 61	h 57	i 63	n 61	e 81	i 40	t 72	w 88	a 97	s 69	t 59	o 82	o 47	w 57	e 79	t 48	t 41	o 51	p 84	l 96	a 81	y 106
Most Frequent	t 85	h 74	e 95	s 93	u 79	n 83	d 94	i 89	w 51	n 58	o 82	t 59	s 61	h 57	i 63	n 61	e 81	z 58	t 72	w 88	a 97	s 69	t 59	o 82	k 64	w 57	e 79	f 55	h 54	c 57	p 84	l 96	a 81	y 106

Table 2: Frequencies of the plaintext letter and most frequent letter in the 1040 ciphertexts.

7 New Variations of Card-Chameleon

Given the biases of Card-Chameleon, we experimented with different variations of the idea of Card-Chameleon to reduce or eliminate these new biases and the other known weaknesses of the cryptosystem. Our goal was also to maintain the relative simplicity of the encryption and decryption processes. In this section, we describe and analyze three variants of Card-Chameleon: Card-Chameleon Face Value, Full-Deck Card-Chameleon, and Full-Deck Card-Chameleon with a Joker.

7.1 Card-Chameleon Face Value

In this variation of Card-Chameleon, the encryption process is identical except for the last two steps. Here, the output card is relocated based on its face value. For example, if the output card is $3\diamondsuit$, it is switched with the third red card above $3\diamondsuit$. Unlike Card-Chameleon, the deck here is treated as a cycle. Thus, this variation has $\frac{(26!)^2}{26} = 26! \cdot 25!$ keyed decks.

Theorem 7.1. *Assuming that the deck is in a random order for each letter, the probability that a letter in the plaintext will encrypt to itself is $\frac{1}{13}$.*

Proof. This follows from Theorem 4.1 since the only change to Card-Chameleon Face Value is the method of mixing the cards after a letter is encrypted. □

Theorem 7.2. *Assuming that the deck is in a random order for each double, the probability that a double in the plaintext will encrypt to a double is $\frac{1}{325}$.*

Proof. Without loss of generality, suppose that we are encrypting AA. There are two types of keyed decks that will encrypt a double to a double. In the first case, $A\spadesuit$ is paired with $A\heartsuit$. In the second case, the two aces are not paired.

Case 1: $A\spadesuit$ and $A\heartsuit$ are paired. Since the aces have a value of 1, a congruent pair (B and R) is above the two aces.

After the first A encrypts to itself, $A\heartsuit$ will switch places with R. The second A will thus map to $A\spadesuit$, which maps to R, which maps to B, which maps to $A\heartsuit$. Thus, the second A also encrypts to itself. Now we count the possibilities. Since each keyed deck is a cycle, we can "cut the deck" so that $A\spadesuit$ is on the bottom. Now, the positions of $A\heartsuit$ and the congruent pairs are forced. There are 25 possible congruent pairs, and the rest of the deck can be permuted in $(24!)^2$ ways. There are $25 \cdot (24!)^2$ keyed decks and the probability of Case 1 occurring is $\frac{25\cdot(24!)^2}{26!\cdot 25!} = \frac{1}{650}$.

Case 2: The two aces are not paired. Also, these two aces are paired with two cards that form a congruent pair. Since aces have a value of 1, $A\spadesuit$ and its paired card must be directly above $A\heartsuit$ and its paired card.

After the first A encrypts to itself, R changes places with $A\heartsuit$. The two aces are now paired, so the second A will encrypt to itself. As in Case 1, we will cut the deck so that $A\heartsuit$ is the second card from the bottom. Now, the position of $A\spadesuit$ and the cards of the congruent pair are forced. There are 25 possible congruent pairs, and the rest of the deck can be permuted in $(24!)^2$ ways. So there are $25 \cdot (24!)^2$ keyed decks and the probability of Case 2 occurring is $\frac{25\cdot(24!)^2}{26!\cdot 25!} = \frac{1}{650}$.

Therefore, the probability of one of these decks occurring is $\frac{50\cdot(24!)^2}{26!\cdot 25!} = \frac{1}{325}$. □

Theorem 7.3. *A double cannot encrypt to a different double.*

Proof. Without loss of generality, suppose that we are encrypting AA. First, we find $A\spadesuit$. The card after it cannot be $A\heartsuit$, or else the first A will encrypt to A. We then find the third card based in what card is above $A\spadesuit$. The card after the third card, which clearly cannot be $A\heartsuit$, is the ciphertext card. We now need to relocate this red card. There are two cases to consider.

Case 1: This red card switches places with the card after $A\spadesuit$. Now, it is impossible for the second A to encrypt to the same letter.

Case 2: This red card does not switch places with the card after $A\spadesuit$. If we refer to this card as B, the second ciphertext character will be the letter represented by B. Again, it is impossible for the second A to encrypt to the same letter. □

Although the statistical bias for doubles has been significantly reduced, the substantial bias for individual letters remains. Furthermore, it is impossible for a double to encrypt to a different double, a pattern that could be exploited by a cryptanalyst.

7.2 Full Deck Card-Chameleon

One obvious drawback of Card-Chameleon is that it requires the deck to alternate black and red cards, so it does not take advantage of the full entropy of a deck of cards. In Full Deck Card-Chameleon, we attempt to utilize the full entropy of the deck. The six-step encryption algorithm is virtually the same and congruent cards disregard the case of the letter. However, there are a few key differences. First, the deck may be keyed with any shuffle of the deck. Also, black cards will represent lowercase letters and the red cards will represent uppercase letters, according to Table 3. Here is the encryption process.

	Spades ($\spadesuit$)												
Card	A	2	3	4	5	6	7	8	9	10	J	Q	K
Letter	a	b	c	d	e	f	g	h	i	j	k	l	m
	Hearts ($\heartsuit$)												
Card	A	2	3	4	5	6	7	8	9	10	J	Q	K
Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
	Clubs ($\clubsuit$)												
Card	A	2	3	4	5	6	7	8	9	10	J	Q	K
Letter	n	o	p	q	r	s	t	u	v	w	x	y	z
	Diamonds ($\diamondsuit$)												
Card	A	2	3	4	5	6	7	8	9	10	J	Q	K
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Table 3: Letter Encoding for Full Deck Card-Chameleon

1. Find the card that represents the plaintext letter.
2. Look at the card above this card.
3. Locate the congruent card in the deck.
4. Look at the card above this card. If this is the top card, look at the bottom card instead. This card represents the ciphertext letter.
5. Switch the ciphertext card with the card on the top of the deck. If it is already on top of the deck, this step can be skipped.
6. Move the top two cards to the bottom of the deck.

The decryption process is a straightforward reversal of the encryption procedure.

1. Find the card that represents the ciphertext letter.
2. Look at the card below this card. If this is the bottom card, look at the top card instead.
3. Locate the congruent card in the deck.

4. Look at the black card below this red card. If this is the bottom card, look at the top card instead. This card represents the plaintext letter.

5. Switch the card in step 1 with the card on the top of the deck. If it is already on top of the deck, this step can be skipped.

6. Move the top two cards to the bottom of the deck.

For example, suppose that we are encrypting `Attack at dawn`. We will use the following deck of cards:

$$[\dots, A\heartsuit, K\heartsuit, \dots, K\spadesuit, 4\spadesuit, \dots, 7\clubsuit, 6\spadesuit, \dots, 6\heartsuit, K\heartsuit, \dots, 4\diamondsuit, 8\spadesuit, 7\spadesuit] \ .$$

First, the `A` signals to us to find $A\heartsuit$. $K\heartsuit$ is above $A\heartsuit$. We now find $K\spadesuit$. The card above $K\spadesuit$ is $4\spadesuit$. Thus, `A` encrypts to `d`. We finish by switching $4\spadesuit$ with the top card, $7\spadesuit$, and moving the top two cards to the bottom. Now the deck is arranged as follows.

$$[8\spadesuit, 4\spadesuit, \dots, A\heartsuit, K\heartsuit, \dots, K\spadesuit, 7\spadesuit, \dots, 7\clubsuit, 6\spadesuit, \dots, 6\heartsuit, K\heartsuit, \dots, 4\diamondsuit]$$

Next, the `t` signals to us to find $7\clubsuit$. $6\spadesuit$ is above $7\clubsuit$. We now find $6\heartsuit$, above which is $K\heartsuit$. Thus, `t` encrypts to `M`. We will then switch $K\heartsuit$ with $4\diamondsuit$ and move the top two cards to the bottom.

To decrypt the `d` after the above encryption, we would locate $4\spadesuit$. $K\spadesuit$ under $4\spadesuit$ would then signal us to find $K\heartsuit$, which would then lead us to $A\heartsuit$, the card that encodes `A`.

Theorem 7.4. *Assuming that the deck is in a random order for each letter, the probability that a letter in the plaintext will encrypt to:*

a. itself and in the same case is $\frac{1}{51} = \frac{49}{2499}$,

b. itself, but in the opposite case, is $\frac{33}{833} = \frac{99}{2499}$, *and*

c. itself, in either case, is $\frac{148}{2499}$.

Proof. Without loss of generality, suppose that we are encrypting `a`. There are three types of keyed decks that will encrypt `a` to either `a` or `A`. The first case has $A\spadesuit$ as the ciphertext card and the last two cases have $A\heartsuit$ as the ciphertext card.

Case 1: $A\spadesuit$ is between two cards that are a congruent pair. An `a` is encoded by $A\spadesuit$, which will lead us to the card above it. Since the cards above and below $A\spadesuit$ are a congruent pair, we will go to the card below $A\spadesuit$ and end up back at $A\spadesuit$. This will encrypt `a` to `a`. To count the possibilities of this, $A\spadesuit$ can be placed in 52 places in the deck. There are 25 congruent pairs that can surround $A\spadesuit$, and there are two ways for each pair to surround the ace. The rest of the deck can be permuted in 49! ways. Thus, there are $52 \cdot 50 \cdot 49!$ such keyed decks and the probability of Case 1 occurring is $\frac{52 \cdot 50 \cdot 49!}{52!} = \frac{1}{51}$. This is the only situation in which a letter encrypts to itself in the same case, establishing part (a).

Case 2: $A\heartsuit$ is directly above $A\spadesuit$. As in the proof of Theorem 4.1, when two paired cards are also a congruent pair, a letter will encrypt to itself. Thus, `a` will encrypt to `A`. To count the possibilities, $A\spadesuit$ and $A\heartsuit$ can be placed in 52 places in the deck. The rest of the deck can be permuted in 50! ways. Thus, there are $52 \cdot 50!$ such keyed decks and the probability of Case 2 occurring is $\frac{52\cdot 50!}{52!} = \frac{1}{51}$.

Case 3: $A\heartsuit$ is not directly above $A\spadesuit$, but the card that is directly above $A\spadesuit$ and the card that is directly below $A\heartsuit$ are a congruent pair. As in the proof of Theorem 4.1, this arrangement will encrypt `a` to `A`. To count the possibilities, $A\spadesuit$ can be placed in 52 places in the deck. Since $A\heartsuit$ cannot be directly above $A\spadesuit$, it can be placed in 50 places in the deck. The two aces can be next to 25 congruent pairs, and there are two ways to do this for each pair. The rest of the deck can be permuted in 48! ways. Thus, there are $52 \cdot 50 \cdot 25 \cdot 2 \cdot 48!$ such keyed decks, so the probability of Case 3 occurring is $\frac{52\cdot 50\cdot 50\cdot 48!}{52!} = \frac{50}{2499}$.

Part (b) follows from Cases 2 and 3. Part (c) also follows. □

By comparison, with perfect encryption, a character would encrypt to any given character with probability $\frac{1}{52}$, so there is a slight bias of a character encrypting to itself. Also, it is slightly more than twice as likely for a letter to encrypt to itself in the opposite case than to encrypt to itself in the same case. These are weaknesses in this variation of the cryptosystem, but it is a vast improvement over Card-Chameleon.

Theorem 7.5. *Assuming that the deck is in a random order for each double, the probability of a double in the plaintext encrypting to itself in the opposite case is* $\frac{199}{129948}$.

Proof. Without loss of generality, suppose that we are encrypting `aa`. There are seven types of keyed decks that will encrypt a double to itself. Since `aa` will be encrypting to `AA`, $A\heartsuit$ will be the output card each time. As shown previously, the first `a` can encrypt to `A` in one of two ways. Either the two aces are the only cards involved, or another congruent pair is involved. Cases 1, 2, and 3 cover the keyed decks in which $A\heartsuit$ is above $A\spadesuit$. In Case 1, both aces are on the top of the deck. In Case 2, the aces are in the middle. In Case 3, $A\spadesuit$ is on top and $A\heartsuit$ is on bottom. Cases 4, 5, 6, and 7 discuss when another congruent pair (X and Y) is involved. We will let X be the card above $A\spadesuit$ and Y be the card below $A\heartsuit$. In Case 4, Y and $A\heartsuit$ are on top of the deck. In Case 5, $A\spadesuit$ and X are on top of the deck. In Cases 6 and 7, $A\spadesuit$ is on top and X is on bottom. Notice that none of the cases have both aces, X, and Y in the middle of the deck. This is because it will be impossible for the second `a` to encrypt to `A`. In addition, although $A\spadesuit$ can be on top and X can be on bottom, we cannot have Y on top and $A\heartsuit$ on bottom.

Case 1: $A\heartsuit$ is above $A\spadesuit$, and they are on the top of the deck. Once $A\spadesuit$ and $A\heartsuit$ are on top, the rest of the deck can be permuted in 50! ways. Thus, there are 50! such keyed decks and the probability of Case 1 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 2: $A\heartsuit$ is above $A\spadesuit$, and they are below the top. Notice that $A\heartsuit$ cannot be second from the top. Also, a congruent pair must be on top. Once $A\spadesuit$ and $A\heartsuit$ are paired with each other, they can be placed in 49 places. Next, 25 congruent pairs can be placed on top, and each of these pairs can be arranged in two ways. Finally, the rest of the deck can be permuted in 48! ways. Thus, there are $49 \cdot 25 \cdot 2 \cdot 48! = 50!$ such keyed decks and the probability of Case 2 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 3: $A\spadesuit$ is on top, and $A\heartsuit$ is on bottom, and the cards that are second from top and bottom are a congruent pair. After the first `a` encrypts to `A`, the two aces will switch places and we will end up with this arrangement on the bottom: $X, A\heartsuit, A\spadesuit, Y$, where X and Y are a congruent pair. Thus, the second `a` will also encrypt to `A`. There can be 25 congruent pairs, and each of these can be arranged in two ways. The rest of the deck can be permuted in 48! ways. Thus, there are $50 \cdot 48!$ such keyed decks and the probability of Case 5 occurring is $\frac{50\cdot 48!}{52!} = \frac{1}{129{,}948}$.

Case 4: Y and $A\heartsuit$ are on the top. After Y and $A\heartsuit$ are placed on top, $A\spadesuit$ and X can be placed in 49 places. Next, there are $25 \cdot 2 = 50$ placements and arrangements of the congruent pair X and Y. Finally, the rest of the deck can be permuted in 48! ways. Thus, there are $49 \cdot 50 \cdot 48! = 50!$ such keyed decks and the probability of Case 4 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 5: $A\spadesuit$ and X are on the top. Once $A\spadesuit$ and X are on top, $A\heartsuit$ and Y can be placed in 49 places. Next, $A\spadesuit$ and $A\heartsuit$ can be paired with 25 congruent pairs, and each of these pairs can be arranged in two ways. Finally, the rest of the deck can be permuted in 48! ways. Thus, there are also $49 \cdot 25 \cdot 2 \cdot 48! = 50!$ such keyed decks and the probability of Case 3 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

The final two cases are variations of the same concept.

Case 6: $A\spadesuit$ is on top, X is on bottom, and Y and $A\heartsuit$ are in the middle. In this case, the card above $A\heartsuit$ and the card under $A\spadesuit$ are a congruent pair (e.g. $\{9\diamondsuit, \cdots, 9\clubsuit, A\heartsuit, 2\spadesuit, \cdots, 2\heartsuit, A\spadesuit\}$). After the first `a` is encrypted, $A\spadesuit$ and $A\heartsuit$ will be next to the second congruent pair, thus causing the second `a` to encrypt to `A`. There are $25 \cdot 2 = 50$ options for the first congruent pair, and there are $24 \cdot 2$ options for the second congruent pair. $A\heartsuit$ and the two cards that it is between can now be placed in 47 positions in the deck. The rest of the deck can be permuted in 46! ways. Thus, there are $50 \cdot 48!$ such keyed decks and the probability of Case 6 occurring is $\frac{50\cdot 48!}{52!} = \frac{1}{129948}$.

Case 7: $A\spadesuit$ is on top, X is on bottom. In this case, Y and $A\heartsuit$ come directly before $A\spadesuit$ (e.g., $\{9\diamondsuit, \cdots, 9\clubsuit, A\heartsuit, A\spadesuit\}$). Case 7 is essentially a modified version of Case 6 in which $A\heartsuit$ and the cards it is between are allowed to shift all the way to the right, thus eliminating the second congruent pair. After the first `a` encrypts to itself, we will end up with $A\spadesuit, A\heartsuit$ on the bottom of the deck. As demonstrated before, this will cause the second `a` to encrypt to itself. After the two aces are placed on top, there are $25 \cdot 2$ options for the congruent pair. The rest of the deck can be permuted in 48! ways. Thus, there are $50 \cdot 48!$ such keyed decks and the probability of Case 7 occurring is $\frac{50\cdot 48!}{52!} = \frac{1}{129948}$.

The total number of keyed decks that will encrypt a double to itself in the opposite case is $4 \cdot 50! + 150 \cdot 48!$ and the probability that a double will encrypt to itself in the opposite case is $\frac{4\cdot 50! + 150\cdot 48!}{52!} = \frac{199}{129948}$. □

Now that we have discussed when a double encrypts to its opposite case, we will consider the remaining three scenarios.

Theorem 7.6. *Assuming that the deck is in a random order for each double,*

1. *the probability of a double encrypting to the same case (e.g.* `aa` *encrypting to* `aa`*) is* $\frac{8}{10829}$*;*

2. *the probability of a double encrypting to the same double such that the first letter is in the same case and the second is in the opposite case (e.g.* `aa` *encrypting to* `aA`*) is* $\frac{1}{1326}$*; and*

3. *the probability of a double encrypting to the same double such that the first letter is in the opposite case and the second is in the same case (e.g.* `aa` *encrypting to* `Aa`*) is* $\frac{25}{64974}$.

Proof. Without loss of generality, suppose that we are encrypting `aa`.

Proof of (1): There are two types of keyed decks that will encrypt `aa` to `aa`. Notice that `a` can only encrypt to itself if $A\spadesuit$ is between a congruent pair (e.g., $\{J\diamondsuit, A\spadesuit, J\clubsuit\}$). In Case 1, $A\spadesuit$ does not change places with another card and thus remains in between the same congruent pair. In Case 2, $A\spadesuit$ does change places, but it ends up between a different congruent pair.

Case 1: $A\spadesuit$ is on top, and the card below $A\spadesuit$ and the bottom card are a congruent pair. There are $25 \cdot 2$ options for the congruent pair and the rest of the deck can be permuted in 49! ways. Thus, there are 50! such keyed decks and the probability of Case 1 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 2: The bottom card and the second card from the top are a congruent pair, and $A\spadesuit$ is between a congruent pair in the middle of the deck. There are $25 \cdot 2$ options for the first congruent pair, and there are $24 \cdot 2$ options for the second congruent pair. $A\spadesuit$ and its congruent pair can be placed in 47 positions in the deck. The rest of the deck can be permuted in 47! ways. Thus, there are $50 \cdot 47 \cdot 48!$ such keyed decks and the probability of Case 2 occurring is $\frac{50 \cdot 47 \cdot 48!}{52!} = \frac{47}{129948}$.

In total, the probability of `aa` encrypting to `aa` is $\frac{50! + 50 \cdot 47 \cdot 48!}{52!} = \frac{8}{10829}$, which establishes (1).

Proof of (2): There are two types of keyed decks that will encrypt `aa` to `aA`. Since the first `a` encrypts to `a`, we know that $A\spadesuit$ must start between a congruent pair. After $A\spadesuit$ changes places, there are two situations. In Case 1, $A\spadesuit$ is moved below $A\heartsuit$. In Case 2, $A\spadesuit$ and $A\heartsuit$ will be next to cards that form a congruent pair.

Case 1: $A\heartsuit$ is on the bottom and $A\spadesuit$ is between a congruent pair. When $A\spadesuit$ is switched with the top card, it will come before $A\heartsuit$. There are $25 \cdot 2$ options for the congruent pair, $A\spadesuit$ and its congruent pair can be placed in 49 places, and the rest of the deck can be permuted in 48! ways. Thus, there are 50! such keyed decks and the probability of Case 1 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 2: $A\spadesuit$ is between a congruent pair, and the card that is below $A\heartsuit$ and the bottom card are a congruent pair. Notice that there are three situations that can occur. First, $A\spadesuit$ and its congruent pair can be on top of the deck. Notice that $A\heartsuit$ cannot be on top. Second, $A\spadesuit$ and its congruent pair are not on top. Third, it is possible for a sequence of the form $\{X, A\spadesuit, Y, A\heartsuit\}$ on the bottom of the deck, where X and Y are a congruent pair.

First, consider when $A\spadesuit$ and its congruent pair are on top of the deck. There are $25 \cdot 2$ options for the first congruent pair and there are $24 \cdot 2$ options for the second congruent pair. $A\heartsuit$ and the card below it can be placed in 47 places. The rest of the deck can be permuted in 46! ways. This enumerates $50 \cdot 48!$ keyed decks.

Second, consider when $A\spadesuit$ and its congruent pair are not on top of the deck. There are $25 \cdot 2$ options for the first congruent pair and there are $24 \cdot 2$ options for the second congruent pair. $A\spadesuit$ with its congruent pair and $A\heartsuit$ with its card can be placed throughout the deck in $2 \cdot \binom{47}{2}$ ways. The rest of the deck can be permuted in 46! ways. This enumerates $50 \cdot 46 \cdot 48!$ keyed decks.

Third, consider when the two aces share the same congruent pair. This occurs when the following configuration is present in the deck: $\{X, A\spadesuit, Y, A\heartsuit\}$. This configuration can only be present in two locations. Either it is on the bottom of the deck, or X is on top and the remaining three cards are on the bottom. In either case, there are $25 \cdot 2$ options for the congruent pair and the rest of the deck can be permuted in 48! ways. This enumerates $2 \cdot 50 \cdot 48!$ keyed decks.

In total, there are $2450 \cdot 48! = 50!$ such keyed decks and the probability of Case 2 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

In total, the probability of `aa` encrypting to `aA` is $\frac{2 \cdot 50!}{52!} = \frac{1}{1326}$, which establishes (2).

Proof of (3): There are two types of keyed decks that will encrypt `aa` to `Aa`. After the first `a` is encrypted, $A\spadesuit$ must end up between a congruent pair, X and Y. However, $A\heartsuit$ is moved after the first encryption, not $A\spadesuit$. This implies that $A\spadesuit$ must begin in between $A\heartsuit$ and either X or Y. Furthermore, Y or X, respectively, must be on top so $A\heartsuit$ will switch places with this card, thus placing $A\spadesuit$ between X and Y. In Case 1, $A\heartsuit$ is above $A\spadesuit$. In Case 2, $A\heartsuit$ is below $A\spadesuit$.

Case 1: $A\heartsuit$ is above $A\spadesuit$, and the card below $A\spadesuit$ and the card on top form a congruent pair (e.g. $[\dots, X, A\spadesuit, A\heartsuit, \dots, Y]$). There are $25 \cdot 2$ options for the congruent pair, the aces and the card below it can be placed in 49 places, and the rest of the deck can be permuted in 48! ways. Thus, there are 50! such keyed decks and the probability of Case 1 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 2: $A\heartsuit$ is below $A\spadesuit$, and the card above $A\spadesuit$ and the top card form a congruent pair. During encryption, $A\spadesuit$ maps to the card above it, which maps to the card on top of the deck. In order for this card to map to $A\heartsuit$, it is must be on the bottom of the deck. Thus, the three card arrangement in discussion is on the bottom of the deck (e.g. $[A\heartsuit, A\spadesuit, X, \cdots, Y]$). There are $25 \cdot 2$ options for the congruent pair and the rest of the deck can be permuted in 48! ways. Thus, there are $50 \cdot 48!$ such keyed decks and the probability of Case 2 occurring is $\frac{50 \cdot 48!}{52!} = \frac{1}{129948}$.

In total, the probability of that `aa` encrypts to `Aa` is $\frac{50! + 50 \cdot 48!}{52!} = \frac{25}{64974}$, which establishes (3). □

7.3 Full Deck Card-Chameleon with a Joker

In this variation of Card-Chameleon, a deck of 52 cards and a joker, $\mathcal{J}$, are used. The encryption process is the same as with Full Deck Card-Chameleon, except that $\mathcal{J}$ is treated as invisible when finding the card "above" a certain card. For example, if we encrypt `b` and the deck contains the order $\{2\spadesuit, \mathcal{J}, 7\diamondsuit, \dots, 7\clubsuit, 8\spadesuit\}$, then we would jump from $2\spadesuit$ to $7\diamondsuit$, find the congruent card, $7\clubsuit$, and then look at $8\spadesuit$ above that to determine the ciphertext letter `h`. The only difference with rearranging the deck order is that instead of switching the ciphertext card with the top card and moving the top two cards to the bottom, the ciphertext card is switched with $\mathcal{J}$.

For example, we will encrypt `Attack at dawn` using the same key as in the previous example, but with a joker as the third card:

$$[\dots, A\heartsuit, K\heartsuit, \dots, K\spadesuit, 4\spadesuit, \dots, 7\clubsuit, 6\spadesuit, \dots, 6\heartsuit, K\heartsuit, \dots, 4\diamondsuit, \mathcal{J}, 8\spadesuit, 7\spadesuit] \ .$$

As before, `A` encrypts to `d`, but instead of switching $4\spadesuit$ with the top card, we switch it with

$\mathcal{J}$, resulting in the following deck:

$$[\ldots, A\heartsuit, K\heartsuit, \ldots, K\spadesuit, \mathcal{J}, \ldots, 7\clubsuit, 6\spadesuit, \ldots, 6\heartsuit, K\heartsuit, \ldots, 4\diamondsuit, 4\spadesuit, 8\spadesuit, 7\spadesuit]\ .$$

Next, the `t` encrypts to `M` as detailed above. We then switch $K\heartsuit$ with $\mathcal{J}$:

$$[\ldots, A\heartsuit, K\heartsuit, \ldots, K\spadesuit, K\heartsuit, \ldots, 7\clubsuit, 6\spadesuit, \ldots, 6\heartsuit, \mathcal{J}, \ldots, 4\diamondsuit, 4\spadesuit, 8\spadesuit, 7\spadesuit]\ .$$

The decryption process is the same as with Full Deck Card-Chameleon, the differences again being the invisibility property of $\mathcal{J}$ and when rearranging the deck, the ciphertext card is switched with $\mathcal{J}$.

Since we are switching a card with a joker as opposed to switching a card with the top card, each keyed deck has become a cycle. Hence, there are still $\frac{53!}{53} = 52!$ ways to key a deck.

Theorem 7.7. *Assuming that the deck is in a random order for each letter, the probability that a letter encrypts to:*

a. itself and in the same case is $\frac{1}{51} = \frac{49}{2499}$*,*

b. itself, but in the opposite case, is $\frac{2}{51} = \frac{98}{2499}$*, and*

c. itself, in either case, is $\frac{3}{51} = \frac{1}{17} = \frac{147}{2499}$*.*

Proof. Without loss of generality, suppose that we are encrypting `a`. The cases can be grouped as follows. Cases 1, 2, and 3 have $A\spadesuit$ as the output card. Cases 4 and 5 have no congruent pairs other than the two aces. Cases 6, 7, and 8 do have another congruent pair.

Case 1: $A\spadesuit$ is between a congruent pair. We will cut the deck so that $A\spadesuit$ and its congruent pair are on bottom. There are 25 possible congruent pairs and each of these can be arranged in two ways. The rest of the deck can be permuted in 50! ways. Thus, there are $50 \cdot 50!$ keyed decks and the probability of Case 1 occurring is $\frac{50 \cdot 50!}{52!} = \frac{25}{1326}$.

Case 2: The deck is arranged as described in Case 1, except that $\mathcal{J}$ is between $A\spadesuit$ and the card above $A\spadesuit$. We will cut the deck so that $A\spadesuit$ with its congruent pair and $\mathcal{J}$ are on bottom. There are 25 possible congruent pairs and each of these can be arranged in two ways. The rest of the deck can be permuted in 49! ways. Thus, there are 50! keyed decks and the probability of Case 2 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 3: The deck is arranged as described in Case 1, except that $\mathcal{J}$ is between $A\spadesuit$ and the card below $A\spadesuit$. We will cut the deck so that $A\spadesuit$ with its congruent pair and $\mathcal{J}$ are on bottom. There are 25 possible congruent pairs and each of these can be arranged in two ways. The rest of the deck can be permuted in 49! ways. Thus, there are 50! keyed decks and the probability of Case 3 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Cases 1-3, establish part (a).

Case 4: $A\spadesuit$ is below $A\heartsuit$. We will cut the deck so $A\spadesuit$ is on the bottom, and the position of $A\heartsuit$ is forced. The rest of the deck can be permuted in 51! ways. Thus, there are 51! keyed decks and the probability of Case 4 occurring is $\frac{51!}{52!} = \frac{1}{52}$.

Case 5: We have the sequence $\{A\spadesuit, \mathcal{J}, A\heartsuit\}$. We will cut the deck so $A\spadesuit$ is on the bottom. The rest of the deck can be permuted in 50! ways. Thus, there are 50! keyed decks and the probability of Case 5 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 6: $A\spadesuit$ is not directly below $A\heartsuit$, and the card above $A\spadesuit$ and the card below $A\heartsuit$ form a congruent pair. We will cut the deck so $A\spadesuit$ is on the bottom. $A\heartsuit$ and the card below it can be placed in 50 places in the deck. There are 25 possible congruent pairs, each of which can be arranged in two ways. The rest of the deck can be permuted in 49! ways. Thus, there are $50 \cdot 50!$ keyed decks and the probability of Case 6 occurring is $\frac{50 \cdot 50!}{52!} = \frac{50}{2652}$.

Case 7: The deck is arranged as described in Case 6, except that $\mathcal{J}$ is between $A\heartsuit$ and the card below $A\heartsuit$. We will cut the deck so $A\spadesuit$ is on bottom. $\mathcal{J}$ and the cards it is between can be placed in 49 places. There are 25 possible congruent pairs, and each of these can be arranged in two ways. The rest of the deck can be permuted in 48! ways. Thus, there are 50! keyed decks and the probability of Case 7 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 8: The deck is arranged as described in Case 6, except that $\mathcal{J}$ is between $A\spadesuit$ and the card above $A\spadesuit$. We will cut the deck so $A\spadesuit$ is on bottom. $A\heartsuit$ with the card above it can be placed in 49 places. There are 25 possible congruent pairs, and each of these can be arranged in two ways. The rest of the deck can be permuted in 48! ways. Thus, Case 8 enumerates 50! keyed decks and the probability of Case 8 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

From Cases 4-8, we find that the probability of a letter encrypting to the opposite case is $\frac{2}{51}$, establishing part (b).

The total number of keyed decks that will encrypt a letter to itself is $51! + 105 \cdot 50!$ and the probability of this occurring is $\frac{51!+105 \cdot 50!}{52!} = \frac{1}{17}$. □

Notice that the probability of a letter encrypting to the same case is the same for both variations of Full Deck Card-Chameleon. Also, it is interesting to note that the probability of a letter encrypting to itself in the opposite case, $\frac{2}{51}$, and in either case, $\frac{1}{17}$, is less than the corresponding probabilities from Theorem 7.4 for the Full Deck version, so the Full Deck with Joker version reduces bias further.

Theorem 7.8. *Assuming that the deck is in a random order for each double, the probability that a double encrypts to itself in the opposite case is* $\frac{1}{442}$.

Proof. Without loss of generality, suppose that we are encrypting `aa`. Cases 1 and 2 describe when the only cards involved are $A\spadesuit$, $A\heartsuit$, and $\mathcal{J}$. Case 3 discusses when another congruent pair is only involved in encrypting the second `a`. Cases 4 and 5 describe when another congruent pair is used to encrypt the first and the second `a`. Finally, Case 6 discusses when another congruent pair is only involved in encrypting the first `a`.

Case 1: We have the card sequence $\{A\spadesuit, A\heartsuit, \mathcal{J}\}$. Since each keyed deck is a cycle, we will cut the deck so that $A\spadesuit$ is on the bottom. The rest of the deck can be permuted in 50! ways. Thus, the probability of Case 1 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 2: We have the card sequence $\{A\spadesuit, \mathcal{J}, A\heartsuit\}$. Since each keyed deck is a cycle, we will cut the deck so that $A\spadesuit$ is on the bottom. The rest of the deck can be permuted in 50! ways. Thus, the probability of Case 2 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 3: $A\spadesuit$ is below $A\heartsuit$, and the card below $\mathcal{J}$ and the card above $A\heartsuit$ are a congruent pair (e.g., $\{K\diamondsuit, \mathcal{J}, \cdots, A\spadesuit, A\heartsuit, K\clubsuit\}$). We will cut the deck so that $A\spadesuit$ is on the bottom. There are 49 positions for $\mathcal{J}$ and the card below it. There are 25 congruent pairs, each of which can be arranged in two ways. The rest of the deck can be permuted in 48! ways. Thus, there are 50! cases and the probability of Case 3 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 4: $A\heartsuit$ is below $\mathcal{J}$, and the card above $A\spadesuit$ and the card below $A\heartsuit$ are a congruent pair (e.g., $\{A\spadesuit, 5\clubsuit, \cdots, 5\diamondsuit, A\heartsuit, \mathcal{J}\}$). We will cut the deck so that $A\spadesuit$ is on the bottom. $A\heartsuit$, the card below it, and $\mathcal{J}$ can be placed in 49 positions in the deck. There are 25 congruent pairs, each of which can be arranged in two ways. The rest of the deck can be permuted in 48! ways. Thus, there are 50! cases and the probability of Case 4 occurring is $\frac{1}{2652}$.

Case 5: $A\heartsuit$ is above $\mathcal{J}$, and the card above $A\spadesuit$ and the card below $\mathcal{J}$ form a congruent pair (e.g., $\{A\spadesuit, 5\clubsuit, \cdots, 5\diamondsuit, \mathcal{J}, A\heartsuit\}$). We will cut the deck so that $A\spadesuit$ is on the bottom. $\mathcal{J}$, with the card below it, and $A\heartsuit$ can be placed in 49 positions in the deck. There are 25 congruent pairs, each of which can be arranged in two ways. The rest of the deck can be permuted in 48! ways. Thus, there are 50! cases and the probability of Case 5 occurring is $\frac{1}{2652}$.

Case 6: $A\spadesuit$ is below $\mathcal{J}$, and the card above $\mathcal{J}$ and the card below $A\heartsuit$ form a congruent pair (e.g., $\{A\spadesuit, \mathcal{J}, 5\clubsuit, \cdots, 5\diamondsuit, A\heartsuit\}$). We will cut the deck so that $A\spadesuit$ is on the bottom. $A\heartsuit$ and the card below it can be placed in 49 positions in the deck. There are 25 congruent pairs, each of which can be arranged in two ways. The rest of the deck can be permuted in 48! ways. Thus, there are 50! cases and the probability of Case 6 occurring is $\frac{1}{2652}$.

The total number of keyed decks that will encrypt a double to itself in the opposite case is $6 \cdot 50!$ and the probability of this occurring is $\frac{6 \cdot 50!}{52!} = \frac{1}{442}$. □

Now that we have discussed when a double encrypts to itself in the opposite case, we will take a look at the remaining three scenarios.

Theorem 7.9. *Assume that the deck is in a random order for each double.*

1. *The probability of a double encrypting to itself in the same case (e.g.,* `aa` *encrypting to* `aa`*) is* $\frac{73}{64{,}974}$.
2. *The probability of a double encrypting to itself such that the first letter is in the same case and the second is in the opposite case (e.g.,* `aa` *encrypting to* `aA`*) is* $\frac{49}{64{,}974}$.
3. *The probability of a double encrypting to itself such that the first letter is in the opposite case and the second is in the same case (e.g.,* `aa` *encrypting to* `Aa`*) is* $\frac{1}{1326}$.

Proof. Without loss of generality, suppose that we are encrypting `aa`.

Proof of (1): There are three types of keyed decks that will encrypt `aa` to `aa`. Recall that in order for a letter to encrypt to its lowercase form, the card that represents the letter in question must be sandwiched in between a congruent pair. Cases 1 and 2 describe when $A\spadesuit$ is between the same congruent pair when the first and the second `a` are encrypted. Case 3 analyzes when $A\spadesuit$ is between two different congruent pairs.

Case 1: $A\spadesuit$ is below $\mathcal{J}$ and $\{A\spadesuit, \mathcal{J}\}$ is between a congruent pair (e.g., as with the card sequence $\{3\clubsuit, A\spadesuit, \mathcal{J}, 3\diamondsuit\}$). We will cut the deck so these four cards are on the bottom. There are 25 possible congruent pairs, each of which can be arranged in two ways. The rest of the deck can be permuted in 49! ways. Thus, there are 50! keyed decks and the probability of Case 1 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 2: $A\spadesuit$ is above $\mathcal{J}$ and $\{\mathcal{J}, A\spadesuit\}$ is between a congruent pair (e.g., as with the card sequence $\{3\clubsuit, \mathcal{J}, A\spadesuit, 3\diamondsuit\}$). We will cut the deck so these four cards are on the bottom.

There are 25 possible congruent pairs, each of which can be arranged in two ways. The rest of the deck can be permuted in 49! ways. Thus, Case 2 enumerates 50! keyed decks and the probability of Case 2 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 3: $A\spadesuit$ and $\mathcal{J}$ are both between two different congruent pairs (e.g.,

$$[\ldots, 2\diamondsuit, A\spadesuit, 2\clubsuit, \ldots, 3\diamondsuit, \mathcal{J}, 3\clubsuit, \ldots]) \ .$$

We will cut the deck so $A\spadesuit$ and the cards surrounding it are on the bottom of the deck. There are $25 \cdot 2$ choices for the first congruent pair, and there are $24 \cdot 2$ congruent choices for the second congruent pair. $\mathcal{J}$ and its congruent pair can be placed in 48 places in the deck, and the rest of the deck can be permuted in 47! ways. Thus, there are $50 \cdot 48 \cdot 48!$ keyed decks and the probability of Case 3 occurring is $\frac{50 \cdot 48 \cdot 48!}{52!} = \frac{4}{10{,}829}$.

The total number of keyed decks that will encrypt `aa` to `aa` is $2 \cdot 50! + 2400 \cdot 48!$ and the probability of this occurring is $\frac{2 \cdot 50! + 2400 \cdot 48!}{52!} = \frac{73}{64{,}974}$.

Proof of (2): There are three types of keyed decks that will encrypt `aa` to `aA`. Notice that since the first `a` encrypts to itself in the same case, $A\spadesuit$ must start out between a congruent pair. Case 1 analyzes when $A\spadesuit$ is subsequently moved above $A\heartsuit$. Case 2 discusses when $A\spadesuit$ is moved above the card that is congruent to the card above $A\heartsuit$. Interestingly, it is possible for this congruent pair to be the same congruent pair surrounding $A\spadesuit$. Case 3 analyzes when this occurs.

Case 1: $A\spadesuit$ is between a congruent pair, and $\mathcal{J}$ is below $A\heartsuit$. We will cut the deck so $A\spadesuit$ and its congruent pair are on the bottom. There are $25 \cdot 2$ options for the congruent pair. $\{\mathcal{J}, A\heartsuit\}$ can then be placed in 49 places in the deck. The rest of the deck can be permuted in 48! ways. Thus, there are 50! keyed decks and the probability of Case 1 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 2: $A\spadesuit$ is between a congruent pair, and $\mathcal{J}$ and $A\heartsuit$ are separate. Also, the card above $\mathcal{J}$ and the card below $A\heartsuit$ are a congruent pair. (For example, consider the shuffle $\{2\diamondsuit, A\spadesuit, 2\clubsuit, \ldots, \mathcal{J}, Q\diamondsuit, \ldots, Q\clubsuit, A\heartsuit\}$.) We will cut the deck so $A\spadesuit$ and its congruent pair are on the bottom. There are $25 \cdot 2$ options for the first congruent pair, and there are $24 \cdot 2$ options for the second congruent pair. Next, the two pairs of cards ($\mathcal{J}$ with its card and $A\heartsuit$ with its card) can be placed in the deck in $2 \cdot \binom{48}{2}$ ways. The rest of the deck can be permuted in 46! ways. Thus, there are $50 \cdot 48 \cdot 48!$ keyed decks and the probability of Case 2 occurring is $\frac{50 \cdot 48 \cdot 48!}{52!} = \frac{4}{10{,}829}$.

Case 3: $A\spadesuit$ is between a congruent pair. Also, these three cards are all above $\mathcal{J}$ and below $A\heartsuit$ (e.g., $\{\mathcal{J}, J\diamondsuit, A\spadesuit, J\clubsuit, A\heartsuit\}$). We will cut the deck so this group of five cards is on the bottom. There are $25 \cdot 2$ choices for the congruent pair and the rest of the deck can be permuted in 48! ways. Thus, there are $50 \cdot 48!$ keyed decks and the probability of Case 3 occurring is $\frac{1}{129{,}948}$.

The total number of keyed decks that will encrypt `aa` to `aA` is $50! + 2450 \cdot 48!$ and the probability of this occurring is $\frac{50! + 2450 \cdot 48!}{52!} = \frac{49}{64{,}974}$.

Proof of (3): There are two types of keyed decks that will encrypt `aa` to `Aa`. Since the second `a` encrypts to itself in the same case, $A\spadesuit$ must be moved between a congruent pair after the first `a` is encrypted. Case 1 describes when the $\{A\spadesuit, A\heartsuit\}$ arrangement is used to encrypt the first `a`. Case 2 describes when a second congruent pair is involved in encrypting the first `a`.

Case 1: $A\spadesuit$ is below $A\heartsuit$, and these two cards are placed in between a congruent pair (e.g. $\{J\diamondsuit A\spadesuit A\heartsuit J\clubsuit\}$). Since $A\heartsuit$ and not $A\spadesuit$ is switched with $\mathcal{J}$, $A\spadesuit$ must start out between a congruent pair. We will cut the deck so this group of four cards is on the bottom. There are 25 possible congruent pairs and each of these can be arranged in two ways. The rest of the deck can be permuted in 49! ways. Thus, there are 50! keyed decks and the probability of Case 1 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

Case 2: $A\heartsuit$ is below $A\spadesuit$, and these two cards are placed in between a congruent pair (e.g., $\{J\diamondsuit, A\heartsuit, A\spadesuit, J\clubsuit\}$). Since $A\spadesuit$ is not switched with $\mathcal{J}$, it must start out between a congruent pair. We will cut the deck so this group of four cards is on the bottom. There are 25 possible congruent pairs, and each of these can be arranged in two ways. The rest of the deck can be permuted in 49! ways. Thus, there are 50! keyed decks and the probability of Case 2 occurring is $\frac{50!}{52!} = \frac{1}{2652}$.

The total number of keyed decks that will encrypt `aa` to `Aa` is $2 \cdot 50!$ and the probability of this occurring is $\frac{2\cdot 50!}{52!} = \frac{1}{1326}$. □

8 Results

Table 4 summarizes our results. OTP stands for one-time pad, CC stands for Card-Chameleon, CCFV stand for the Face Value variation, CCFD stands for the Full Deck variation, and CCFDJ stands for the Full Deck with Joker variation. The probabilities listed are the probabilities that a given cipher will encrypt a letter to itself and a double to itself. Notice that with the Full Deck variations, we consider a letter encrypting to itself as a different case as still being itself.

Cryptosystem	**OTP**	**CC**	**CCFV**	**CCFD**	**CCFDJ**
Singles	0.03846	0.07692	0.07692	0.05922	0.05882
Doubles	0.00148	0.00592	0.00308	0.00303	0.00489

Table 4: Comparing single-letter and double-letter biases of Card-Chameleon and variants.

Each of our three variations of Card-Chameleon improves on the biases of Card-Chameleon, but none of them achieves the perfection of the One-Time Pad. Full-Deck Card-Chameleon reduced the bias of doubles the most, but Full-Deck Card-Chameleon with a Joker reduced the bias for singles the most. This bias is certainly the most important to reduce, so of the variations, CCFDJ is the most secure.

9 Conclusions and Future Work

In addition to being secure, a good stream or block cipher using a deck of cards should be resistant to mistakes by being fast to implement and by not using arithmetic that cannot be done mentally. The latter two qualities make Card-Chameleon attractive, but its major shortfalls are its significant statistical biases. Our Full-Deck versions reduced these biases, but did not completely eliminate them. Future work may attempt to further reduce these biases without overly complicating the algorithm.

Acknowledgments: We gratefully acknowledge support for this project through the Kutztown University Bringing Experience About Research in Summer (KU BEARS) program. We also thank the reviewers and editors for their thoughtful reviews, encouraging words, and for providing very constructive feedback that helped us significantly improve the paper.

References

[1] R.A. Fisher and F. Yates, *Statistical tables for biological, agricultural and medical research (3rd ed.)* (1948), London: Oliver & Boyd, 26–27.

[2] M. McKague, Design and Analysis of RC4-like Stream Ciphers, *Master Thesis — University of Waterloo* (2005). `http://hdl.handle.net/10012/1141`.

[3] R. Rivest and J. Schuldt, Spritz — a spongy RC4-like stream cipher and hash function, *IACR Cryptol.* (2016), 856. `https://eprint.iacr.org/2016/856`.

[4] B. Schneier, *The Solitaire Encryption Algorithm* (1999), `http://www.schneier.com/solitaire.html`.

[5] K. Spinar, *Text.cs* (2017), `https://github.com/alipha/CardCrypto/blob/master/CardCrypto/Test.cs`.

[6] N. Stephenson, *Cryptonomicon* (1999), Avon Books.

[7] A. Toponce, *Playing Card Ciphers* (2018), `https://aarontoponce.org/wiki/crypto/card-ciphers`.