Encryption with Playing Cards: An Introduction to Solitaire Encryption

Alpheus Madsen

Provo Linux User's Group
Tuesday, 20 February 2018

Background: Why Solitaire?

Neil Stevenson's *Cryptonomicron*

Background: Why Solitaire?

Neil Stevenson's *Cryptonomicron*

- WWII cryptography

Background: Why Solitaire?

Neil Stevenson's *Cryptonomicron*

- WWII cryptography
- Juxtaposed with modern day cryptography

Background: Why Solitaire?

Neil Stevenson's *Cryptonomicron*

- WWII cryptography
- Juxtaposed with modern day cryptography
- Modern day protagonists dealing with tyranny

Background: Why Solitaire?

Neil Stevenson's *Cryptonomicron*

- WWII cryptography
- Juxtaposed with modern day cryptography
- Modern day protagonists dealing with tyranny
- A fun introduction to cryptography

Background: Why Solitaire?

Neil Stevenson's *Cryptonomicron*

- WWII cryptography
- Juxtaposed with modern day cryptography
- Modern day protagonists dealing with tyranny
- A fun introduction to cryptography
- Normalizing cryptography

Background: Why Solitaire?

Solitaire's Goals

Background: Why Solitaire?

Solitaire's Goals

- Strong Encryption — avoiding "Security through Obscurity"

Background: Why Solitaire?

Solitaire's Goals

- Strong Encryption — avoiding "Security through Obscurity"
- Assumes computer is not available

Background: Why Solitaire?

Solitaire's Goals

- Strong Encryption — avoiding "Security through Obscurity"
- Assumes computer is not available
- Uses non-incriminating tools

Background: Why Solitaire?

Solitaire's Goals

- Strong Encryption — avoiding "Security through Obscurity"
- Assumes computer is not available
- Uses non-incriminating tools
  — After all, what's so incriminating about a deck of cards?

Security Concerns

Concerns with Solitaire's Security and Practicality

Security Concerns

Concerns with Solitaire's Security and Practicality

- Output key stream should *never* be re-used

Security Concerns

Concerns with Solitaire's Security and Practicality

- Output key stream should *never* be re-used
- Biases in output — algorithm favors some numbers over others

Security Concerns

Concerns with Solitaire's Security and Practicality

- Output key stream should *never* be re-used
- Biases in output — algorithm favors some numbers over others
- Algorithm is error prone

Security Concerns

Concerns with Solitaire's Security and Practicality

- Output key stream should *never* be re-used
- Biases in output — algorithm favors some numbers over others
- Algorithm is error prone
  - Messages should be kept short: use abbreviations and slang

Security Concerns

Concerns with Solitaire's Security and Practicality

- Output key stream should *never* be re-used
- Biases in output — algorithm favors some numbers over others
- Algorithm is error prone
  - Messages should be kept short: use abbreviations and slang (Twitter FTW!)

Security Concerns

Concerns with Solitaire's Security and Practicality

- Output key stream should *never* be re-used
- Biases in output — algorithm favors some numbers over others
- Algorithm is error prone
  - Messages should be kept short: use abbreviations and slang (Twitter FTW!)
  - Encryption/Decryption by hand needs to be double-checked

Security Concerns

Concerns with Solitaire's Security and Practicality

- Output key stream should *never* be re-used
- Biases in output — algorithm favors some numbers over others
- Algorithm is error prone
  - Messages should be kept short: use abbreviations and slang (Twitter FTW!)
  - Encryption/Decryption by hand needs to be double-checked
  - Backup card deck(s) highly advisable!

Security Concerns

Concerns with Solitaire's Security and Practicality

- Output key stream should *never* be re-used
- Biases in output — algorithm favors some numbers over others
- Algorithm is error prone
  - Messages should be kept short: use abbreviations and slang (Twitter FTW!)
  - Encryption/Decryption by hand needs to be double-checked
  - Backup card deck(s) highly advisable!
  - Should use computer whenever possible

Solitaire's Algorithm

Encoding Messages

Solitaire's Algorithm

Encoding Messages

- Start with a message

HI! I'm here to help!

Solitaire's Algorithm

Encoding Messages

- Start with a message
- Break message into 5-block groups

HIXIX MXHER ETOXH ELPXX

Solitaire's Algorithm

Encoding Messages

- Start with a message
- Break message into 5-block groups
- Convert to numbers

HIXIX MXHER ETOXH ELPXX

8 9 24 9 24   13 24 8 5 18   5 20 15 24 8   5 12 16 24 24

Solitaire's Algorithm

Encoding Messages

- Start with a message
- Break message into 5-block groups
- Convert to numbers
- Add stream to numbers modulo 26

phrase:	8	9	24	9	24	13	24	8	5	18	5	20	15	24	8	5	12	16	24	24
stream:	7	26	5	4	17	15	15	7	17	10	7	16	8	5	20	17	18	6	3	22
code:	15	9	3	13	15	2	13	15	22	2	12	10	23	3	2	22	6	22	1	20

Solitaire's Algorithm

Encoding Messages

- Start with a message
- Break message into 5-block groups
- Convert to numbers
- Add stream to numbers modulo 26
- Convert back to letters

15 9 3 13 15   2 13 15 22 2   12 10 23 3 2   22 6 22 1 20
O I C M O   B M O V B   L J W C B   V F V A T

Solitaire's Algorithm

Decoding Messages

Solitaire's Algorithm

Decoding Messages

- Start with the encrypted message

OICMO BMOVB LJWCB VFVAT

Solitaire's Algorithm

Decoding Messages

- Start with the encrypted message
- Convert to numbers

O I C M O B M O V B L J W C B V F V A T

15 9 3 13 15 2 13 15 22 2 12 10 23 3 2 22 6 22 1 20

Solitaire's Algorithm

Decoding Messages

- Start with the encrypted message
- Convert to numbers
- Subtract stream from numbers modulo 26

code:	15	9	3	13	15	2	13	15	22	2	12	10	23	3	2	22	6	22	1	20
stream:	7	26	5	4	17	15	15	7	17	10	7	16	8	5	20	17	18	6	3	22
phrase:	8	9	24	9	24	13	24	8	5	18	5	20	15	24	8	5	12	16	24	24

Solitaire's Algorithm

Decoding Messages

- Start with the encrypted message
- Convert to numbers
- Subtract stream from numbers modulo 26
- Convert to letters

8 9 24 9 24 13 24 8 5 18 5 20 15 24 8 5 12 16 24 24

H I X I X M X H E R E T O X H E L P X X

Solitaire's Algorithm

Decoding Messages

- Start with the encrypted message
- Convert to numbers
- Subtract stream from numbers modulo 26
- Convert to letters

Fun Fact

If you practice enough, you can do letter arithmetic in your head! (eg, A + A = B, T + Q = K, etc)

Solitaire's Algorithm

Decoding Messages

- Start with the encrypted message
- Convert to numbers
- Subtract stream from numbers modulo 26
- Convert to letters

Fun Fact

If you practice enough, you can do letter arithmetic in your head! (eg, A + A = B, T + Q = K, etc)

Indeed: Ideally, you should be able to do *all* of this in your head, so you don't have incriminating notes and stuff that can be used to decrypt messages laying about…

Solitaire's Algorithm

Obtaining a stream of numbers

Solitaire's Algorithm

Obtaining a stream of numbers

1. Find the $\mathbb{A}$ Joker. Move it *one* card *towards* you.

Solitaire's Algorithm

Obtaining a stream of numbers

1. Find the $\mathbb{A}$ Joker. Move it *one* card *towards* you.
2. Find the $\mathbb{B}$ Joker. Move it *two* cards *towards* you.

Solitaire's Algorithm

Obtaining a stream of numbers

1. Find the $\mathbb{A}$ Joker. Move it *one* card *towards* you.
2. Find the $\mathbb{B}$ Joker. Move it *two* cards *towards* you.
3. Perform a triple cut: swap all the cards before the first Joker (whatever Joker that might be) with all the cards after the second Joker.

Solitaire's Algorithm

Obtaining a stream of numbers

1. Find the $\mathbb{A}$ Joker. Move it *one* card *towards* you.
2. Find the $\mathbb{B}$ Joker. Move it *two* cards *towards* you.
3. Perform a triple cut: swap all the cards before the first Joker (whatever Joker that might be) with all the cards after the second Joker.
4. Perform a count cut: look at the first card *towards* you, and convert it to a number from 1 to 53. Count from the card *furthest from* you. DO NOT change the order. Take those cards, and put them *under* the first card.

Solitaire's Algorithm

Obtaining a stream of numbers

1. Find the $\mathbb{A}$ Joker. Move it *one* card *towards* you.
2. Find the $\mathbb{B}$ Joker. Move it *two* cards *towards* you.
3. Perform a triple cut: swap all the cards before the first Joker (whatever Joker that might be) with all the cards after the second Joker.
4. Perform a count cut: look at the first card *towards* you, and convert it to a number from 1 to 53. Count from the card *furthest from* you. DO NOT change the order. Take those cards, and put them *under* the first card.
5. Find the output card: look at the card *furthest from* you. Count down (ie, *towards* you) that many cards — the furthest card counts as one — and convert the card that you "land" on to a number, 1 to 26. This doesn't change the deck.

Solitaire's Algorithm

Obtaining a stream of numbers

1. Find the $\mathbb{A}$ Joker. Move it *one* card *towards* you.
2. Find the $\mathbb{B}$ Joker. Move it *two* cards *towards* you.
3. Perform a triple cut: swap all the cards before the first Joker (whatever Joker that might be) with all the cards after the second Joker.
4. Perform a count cut: look at the first card *towards* you, and convert it to a number from 1 to 53. Count from the card *furthest from* you. DO NOT change the order. Take those cards, and put them *under* the first card.
5. Find the output card: look at the card *furthest from* you. Count down (ie, *towards* you) that many cards — the furthest card counts as one — and convert the card that you "land" on to a number, 1 to 26. This doesn't change the deck.

Repeat these steps (without rekeying the deck) until you have

Solitaire's Algorithm

Keying the Deck

Solitaire's Algorithm

Keying the Deck

- Random shuffling (requires copy or two of deck)

Solitaire's Algorithm

Keying the Deck

- Random shuffling (requires copy or two of deck)
- Using a Bridge column

Solitaire's Algorithm

Keying the Deck

- Random shuffling (requires copy or two of deck)
- Using a Bridge column
- Using a phrase and the algorithm itself

Solitaire's Algorithm

Keying the Deck

- Random shuffling (requires copy or two of deck)
- Using a Bridge column
- Using a phrase and the algorithm itself
  (Convert phrase to a series of numbers, and for every step in the phrase, repeat step 4 — the count cut — with that number in the phrase)

Solitaire's Algorithm

Keying the Deck

- Random shuffling (requires copy or two of deck)
- Using a Bridge column
- Using a phrase and the algorithm itself
  (Convert phrase to a series of numbers, and for every step in the phrase, repeat step 4 — the count cut — with that number in the phrase)

  Note that this is a good way to practice the algorithm...

Variations and Alternatives to Solitaire

Variations and Alternatives to Solitaire

Variations and Alternatives to Solitaire

Variations and Alternatives to Solitaire

- Letters *and* Punctuation

Variations and Alternatives to Solitaire

Variations and Alternatives to Solitaire

- Letters *and* Punctuation
- One Time Pad?

Variations and Alternatives to Solitaire

Variations and Alternatives to Solitaire

- Letters *and* Punctuation
- One Time Pad?
- Various stream ciphers

Variations and Alternatives to Solitaire

Variations and Alternatives to Solitaire

- Letters *and* Punctuation
- One Time Pad?
- Various stream ciphers
- Public/Private Key Encryption?

Questions

Any Questions?

Resources

- Bruce Schneier's Description:
  - https://www.schneier.com/academic/solitaire/
  - Problems With "Solitaire"
    http://www.ciphergoth.org/crypto/solitaire/
- Aaron Toponce's resources
  - https://pthree.org/2014/09/15/playing-card-ciphers/
  - Card Cipher Wiki Page
    https://arrontoponce.org/wiki/card-ciphers
- DiceWare
  http://world.std.com/ reinhold/diceware.html