SECURE SECRET SANTA 2.0

PROTOCOL WALKTHROUGH

INTRODUCTION

- Secure Secret Santa 2.0 (SSS2) is an alternative to the first version of the Secure Secret Santa Protocol that does not require a trusted central system to perform the derangement and encrypt the each participant's assigned recipient.
- It is **trustless** and **decentralised** – each participant performs some part of the computations in such a way that if participants collude, they can obtain no more information than they already know.
- In order to meet these requirements, some more complexity is introduced. It also becomes possible again to have fixed points in the resulting permutation, i.e. people drawing there own names. **In this case, the protocol must be restarted from step 1.** However, the chance of this happening is only approx. 36.8%, and so the chance of needed to restart more than 3 times is less than 5%.
- Because of the potential complexity, in this document we follow Alice, Bob, Charlotte, and Dennis as they use SSS2 to establish a Secret Santa assignement.

STEP 0: PREPARATION

- All the participants have navigated to this website, or have agreed to use their own implementation.
- They have also agreed on an eliptic curve group (`CURVE`) and cryptographic hash function (`HASH_FUCNTION`) – these are the cryptographic primitives that the SSS2 protocol is built on.
- They have also agreed on a **shared** and **authenticated** means of communication to disseminate public information as required by the protocol. They have chosen to use a WhatsApp group chat.

STEP 1: GENERATING AND SHARING KEYS

- Having run cells 1, 2, and 3 (which must be done before running any other cell), each participant runs cell 4 to generate a public/private key pair. They publish their **public key**, and record their **private key** somewhere secure.
- Here's what **Alice** sees in the group chat.
- She's made a note of her private key.

```
MY PRIVATE KEY:
A5FaXPzkfllAhSxJstT/Ojg1
p5A7u/sX+gtpRrC2ma0
```

Bob

XX/Ox1Tspis2ILLzgf277gQYpVU4OsxtiCWJOYV5IH0XV9X
VrrMIKiNp5rT6awbDSJw0dDgDIDQvR7bhFl/P4E

Charlotte

DXT7iwuBeFdAEVQdx+r2gE5eY3JoaQYiPyC64iQbKKAlpw
GmRHn3e68VxXH9gzO3hhHcYF+zacIdat2r5pLSw4

Q0Jr6JQ6knfhJJoYcHqZexhF2LoSJZ4odMaWKX76P0M8sQ+
QFjiny/j5LlmRM5ugkFEZhxGmBZeqo1mdd3U3kE

Dennis

J2oslkxsU01IJf2j9cZp8rU5qns9VaynZyjmJz3jIz8EcfynpD6IG8/f
auvlLmnrb4GJoqMwuRGIdotJ1ugBR8

STEP 2: BUILD INITIAL LIST

- Charlotte has taken it upon herself to be the one to compile the initial list (`LIST_0`)
- She fills in the details from the group chat into cell 5:

```
NAME_KEY_PAIRS = [
    ("Bob", "XX/Ox1Tspis2ILLzgf277gQYpVU4OsxtiCWJOYV5IH0XV9XVrrMIKiNp5rT6awbDSJw0dDgDIDQvR7bhFl/P4E"),
    ("Charlotte", "DXT7iwuBeFdAEVQdx+r2gE5eY3JoaQYiPyC64iQbKKAIpwGmRHn3e68VxXH9gzO3hhHcYF+zacIdat2r5pLSw4"),
    ("Alice", "Q0Jr6JQ6knfhJJoYcHqZexhF2LoSJZ4odMaWKX76P0M8sQ+QFjiny/j5LlmRM5ugkFEZhxGmBZeqo1mdd3U3kE"),
    ("Dennis", "J2oslkxsU01lJf2j9cZp8rU5qns9VaynZyjmJz3jIz8EcfynpD6IG8/fauvlLmnrb4GJoqMwuRGldotJ1ugBR8")
]
```

- She shares the following output in the group chat:

```
LIST_0
0: [axfR8uEsQkf4vOblY6RA8ncDfYEt6zOg9KE5RdiYwpYT+NC4v4af5uO5+tKfA+eFivOM1drMV7Oy7ZAaDe/UfU]
1: [Q0Jr6JQ6knfhJJoYcHqZexhF2LoSJZ4odMaWKX76P0M8sQ+QFjiny/j5LlmRM5ugkFEZhxGmBZeqo1mdd3U3kE] (Alice)
2: [XX/Ox1Tspis2ILLzgf277gQYpVU4OsxtiCWJOYV5IH0XV9XVrrMIKiNp5rT6awbDSJw0dDgDIDQvR7bhFl/P4E] (Bob)
3: [DXT7iwuBeFdAEVQdx+r2gE5eY3JoaQYiPyC64iQbKKAIpwGmRHn3e68VxXH9gzO3hhHcYF+zacIdat2r5pLSw4] (Charlotte)
4: [J2oslkxsU01lJf2j9cZp8rU5qns9VaynZyjmJz3jIz8EcfynpD6IG8/fauvlLmnrb4GJoqMwuRGldotJ1ugBR8] (Dennis)
```

STEP 3: SHUFFLE THE LIST

- `LIST_0` assigns each participant a **participant number** (alphabetically), so Alice is 1, Bob is 2, etc.
- Participant N must produce list N by copying list $N-1$ into cell 6, and sharing the result.
- Since Alice is participant 1, she copies `LIST_0` and runs cell 6 to produce `LIST_1`, which she publishes.

```
LIST = """
LIST_0
0: [axfR8uEsQkf4vOblY6RA8ncDfYEt6zOg9KE5RdiYwpYT+NC4v4af5uO5+tKfA+eFivOM1drMV7Oy7ZAaDe/UfU]
1: [Q0Jr6JQ6knfhJJoYcHqZexhF2LoSJZ4odMaWKX76P0M8sQ+QFjiny/j5LlmRM5ugkFEZhxGmBZeqo1mdd3U3kE] (Alice)
2: [XX/Ox1Tspis2ILLzgf277gQYpVU4OsxtiCWJOYV5IH0XV9XVrrMIKiNp5rT6awbDSJw0dDgDIDQvR7bhFl/P4E] (Bob)
3: [DXT7iwuBeFdAEVQdx+r2gE5eY3JoaQYiPyC64iQbKKAIpwGmRHn3e68VxXH9gzO3hhHcYF+zacIdat2r5pLSw4] (Charlotte)
4: [J2oslkxsU01lJf2j9cZp8rU5qns9VaynZyjmJz3jIz8EcfynpD6IG8/fauvlLmnrb4GJoqMwuRGldotJ1ugBR8] (Dennis)
"""
```

```
LIST_1
0: [Lk716Q/fRc6KCzLMzGvvbpJ1R2zZi6sxPDksis2SsgI6jeZeOCwsfRaMmfs+l0tYwZN5yWyS/ESF5RYT5MebQk]
1: [HdQNvkbj6pzUSIEpLwrn2xlvfLAd7V5Vce+CQLUcZVw/UlwT79DDPsbEksnRqCStSnqD11kETYVSCtqtmuIdT0]
2: [AsVfBcbcwo/6+sM5kgFdk62jpKEJ+MHIA2exy0++62cCBE6i3DW4xMaVYiDnYLqKzozh6rh707q8ea/ekqN+/4]
3: [Zv5NX34sAlUFsRvAZVrSVhrIw5sryTpiR0MwaAg1C+sBn7AcGxo5Vu2CGKLicpe+/aNcDjpLSJrKdO6Be+f9do]
4: [WzyCSq+P7Zy4Z9Y6JkqE9zYIaZy6QPPxXSfRH+eZ1nM72FqchsyfqLaypPguUltnVdexCb1cFKu/brYNumqflc]
```

STEP 3: SHUFFLE THE LIST

- The other participants do the same as Alice, following the order of their participant numbers, and publishing the results to the group chat.
- Here's what Alices sees (messages truncated to fit):

```
LIST_1
0:[Lk716Q/fRc6KCzLMzGvvbpJ1R2zZi6sxPDksis2SsgI6jeZeOCwsfRaMm
fs+l0tYwZN5yWyS/ESF5RYT5MebQk]...
```

Bob

```
LIST_2
0:[Ib29ccc0pT6m2dMs+ZWX5jY/iXZyCDTotqUB7dzwq5I+hpuEC7lSh8qBD
5m246y0eeJLGlOuGI5KqZldsIcs5c]...
```

Charlotte

```
LIST_3
0:[U11m+1JNBM0pB8iQjc1ycib1+k0d+/Poi1QuC2/V9jslgtLGewd9U3j3h
Lfdt9/1l1uad/IpjtJbBc+o2AGevE]...
```

Dennis

```
LIST_4
0:[GLMdxnQX17THxigGBMBVF1x1famTQNAv1TOt2Kk8m9oVBYZhI8F+1RDj8
lBmlVGhbU6dCNErElLH9cDE6EEmbs]
```

STEP 4: IDENTIFYING SECRET NUMBER

- Once all participants have shuffled the list, and `LIST_N` has been shared (`N` is the number of participants), each participant can use their private key to discover which line of the list derives from their public key.
- The number of this line is the participant's **secret number**.
- Alice copies `LIST_N` and her private key into cell 7 before running it. She then records her secret number.

```
# Private Key
sk = "A5FaXPzkfllAhSxJstT/Ojg1p5A7u/sX+gtpRrC2ma0"

# LIST_N
L = """
LIST_4
0: [GLMdxnQX17THxigGBMBVF1x1famTQNAv1TOt2Kk8m9oVBYZhI8F+1RDj8lBmlVGhbU6dCNErElLH9cDE6EEmbs]
1: [16DyKR5VaZ3lIc1nFJ4+5Sg0T1TXkbz2AvWBzrLoIFsulenVDj0Q7hGdqqfHmRS+/28EFYjSDlaVirsGqeu1o0]
2: [Byd6FS1L7iRnV6aEKV6+e7p6MMvYYrEOtBBV+vSDePEsBKMJs/8QbPCHs+CtlXbziu6q6JkRdKHGOx9w4vWgjQ]
3: [q2mZEc/oh74GbUYLjAfgIwV6/MtQVPA3EyJu3zqX1jo7Vu8VoOICYISw0dGvdkwQsctr6sawbtsAdoHpTxBH4E]
4: [ztdneLZZiiG9OVymZf2wy88uDsWWKyOAK8c5LaugQiIvLunnTGzWjEyj58pvQpnoopgjDIhcTnMPEM4KFeQMjM]
"""
```

Your secret number is 3

MY SECRET NUMBER: 3

STEP 5: SHARING PROMISES & SEEDS

- The final participant to shuffle the list can choose which secret number they get. Therefore, before using the secret numbers to assign recipients, the secret numbers need to be secretly shuffled!
- Each participant runs cell 7 to generate a seed to generate a shuffle and a promise for that shuffle.
- Everyone shares their **shuffle promises** first.
- Once all the promises are shared, everyone shares their **shuffle seeds**.
- Here's what Alice sees:

Dennis

```
Fjg5bH7qeftP1bgmV0iQX+tFUKLi2WuntOMARNJAlZ4
```

```
vfgcSyzJ+2BP8L9EBhhM7PoEEGw0WgfWZsOsx/J2RKI
```

Charlotte

```
srFUUIYL102Tk4iEoPabc0jUqbmGKC9+p0Qb6VCLkXA
```

Bob

```
X9ARCGz5/hUSU+mdRtedj+eeclz9Uh8kcDaSnWlFCAE
```

Ok seeds now:

```
xkihnJhYzr1/mHYoFjGMk7QHKysB2c5xl4mcRLwbxuI
```

Charlotte

```
av0UvckHPS26uiktkDGzdeQ93COmMgfQ6tgruP8U0bQ
```

Dennis

```
KF86kSv9FAU2ROdz0FlSSv3nJY1416peXe/UAvSxIAA
```

```
SYYVcuN+4aYskq9sWLr4A/EjXsNF6W3PAxdbhY8HF+c
```

STEP 6: DETERMINING RECIPIENT NUMBER

- Each participant must now enter lists of promises and seeds, **ordered by participant number**, into cell 8, along with their secret number.
- Running cell 8 with this information produces the **recipient number**, which is the participant number of the person for whom you are buying a gift!
- Here's what that looks like for Alice:

STEP 9: RESOLVING CLASHES

- Oh no! Alice has a **clash** – since she is participant number one (see `LIST_0` again to check), she has been assigned herself as a recipient.
- She should alert the other participants as soon as possible, and publish her **private key** so that other participants can find out her secret number to verify that she is telling the truth.
- To continue the protocol, return to step 1.

```
promises = """
vfgcSyzJ+2BP8L9EBhhM7PoEEGw0WgfWZsOsx/J2RKI
X9ARCGz5/hUSU+mdRtedj+eeclz9Uh8kcDaSnWlFCAE
srFUUIYL102Tk4iEoPabc0jUqbmGKC9+p0Qb6VCLkXA
Fjg5bH7qeftP1bgmV0iQX+tFUKLi2WuntOMARNJAlZ4
"""

seeds = """
SYYVcuN+4aYskq9sWLr4A/EjXsNF6W3PAxdbhY8HF+c
xkihnJhYzr1/mHYoFjGMk7QHKysB2c5xl4mcRLwbxuI
av0UvckHPS26uiktkDGzdeQ93COmMgfQ6tgruP8U0bQ
KF86kSv9FAU2ROdz0FlSSv3nJY1416peXe/UAvSxIAA
"""

secret_number = 3
```

```
Recipient Number: 1
```