Backgrounder:
Running the computation
Backgrounder:
Keys / encryption / decryption
Decision: Key holder?

- **Step 1: Generate keys**
  - Login
  - Create key
  - Secure with password
  - Store on server or locally

- **Step 2: Encrypt and upload data**
  - Login (if time delayed)
  - Upload data into browser
  - Encrypt and send to MIT

- **Step 3: Decrypt the result**
  - Login (if time delayed)
  - Enter password to use private key to decrypt results
Suggestion on holding keys

Our computation can be done in one sitting, so I suggest we make everyone a keyholder and go through it together.
Step 1: Generating the keys

- Start by clicking on “Perform Keyholder Role”
- Put in a strong password that is used to encrypt your private key for storage
- Select where to store the key (MIT server or your hard drive). If you choose the local option, make sure to put it in a place you will be able to find it again easily. Otherwise, we cannot decrypt any of the results.

Click “Generate Key” to complete.
Step 2: Uploading and encrypting the data

- There are two important steps here
  - **Part 1:**
    - Upload the spreadsheet into the browser
  - **Part 2:**
    - Encrypt input and send to MIT

Don’t forget to click to encrypt and upload.
Step 2: Confirmations

Confirmation Part 1: Data in browser

Welcome to SCRAM.

Spreadsheet Uploaded

- Upload Spreadsheet to your browser
- Encrypt Input and send to MIT
- Return to Home Page

Confirmation Part 2: Data uploaded

Welcome to SCRAM

- Data Accepted

Welcome!

You are participating in Cambridge Comp (#11) - Mar 2021.

You are entering data

Enter Data

Reload  Logout
Step 3: Decrypting the results

- Put in the password to decrypt your private key and then click “Decrypt Your Share” to perform the partial decryption of the result and send it to be combined with others.
Credentials

(Let us know how you want to receive them)
Thank you