



SCRAM

Secure Cyber Risk Aggregation and Measurement



Internet Policy Research Initiative
Massachusetts Institute of Technology

Backgrounder:

Running the computation

Backgrounder:

Keys / encryption / decryption

Decision: Key holder?



Key holder and
data provider

Data provider
only

- **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

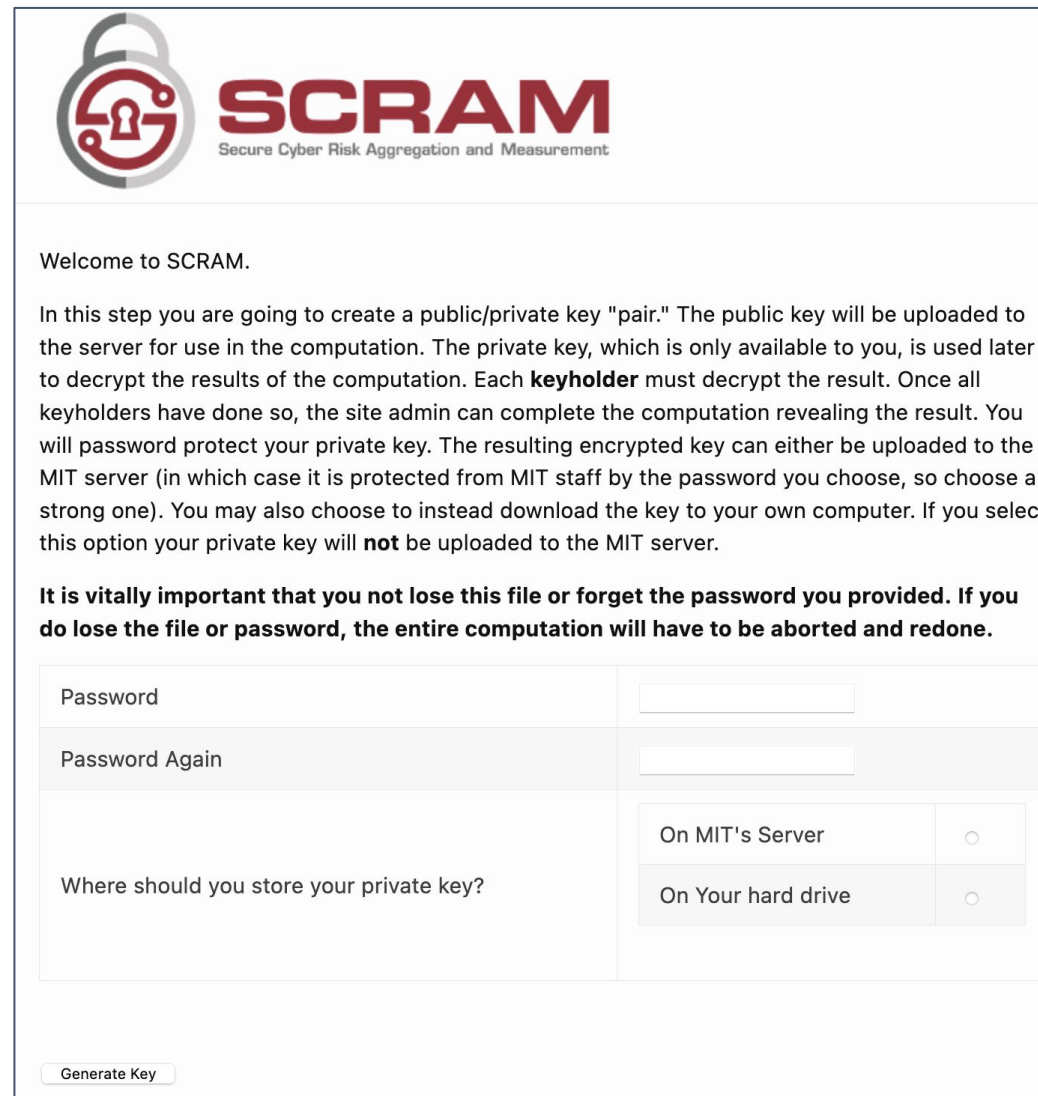
Suggestion on holding keys

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

You are a Key Holder	Perform Keyholder Role
You are entering data	Enter Data

- 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 the results



The screenshot shows the SCRAM web interface. At the top left is the SCRAM logo (a padlock with a keyhole) and the text "SCRAM Secure Cyber Risk Aggregation and Measurement". Below the logo, it says "Welcome to SCRAM." followed by a paragraph explaining the key generation process. A bold warning states: "It is vitally important that you not lose this file or forget the password you provided. If you do lose the file or password, the entire computation will have to be aborted and redone." Below this is a form with three sections: "Password" and "Password Again" each with a text input field; "Where should you store your private key?" with two radio button options: "On MIT's Server" and "On Your hard drive". At the bottom left of the form is a "Generate Key" button. A red arrow points from the text "Click 'Generate Key' to complete" to this button.


Click "Generate Key" to complete



Step 2: Uploading and encrypting the data

You are a Key Holder	Perform Keyholder Role
You are entering data	Enter Data

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



Welcome to SCRAM.


[Upload Spreadsheet to your browser](#)

[Encrypt Input and send to MIT](#) ← Don't forget to click to encrypt and upload

[Return to Home Page](#)

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

You are a Key Holder	Perform Keyholder Role
You are entering data	Enter Data

- 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



Welcome to SCRAM.

At this point all of the data has been entered and you should enter your password which will be used to decrypt your private key and perform your portion of the results decryption. If you chose to store your private key on your own computer, you should select the file you stored it in below (use the "Upload Private Key" button). Click "Decrypt Your Share" to complete the operation.

Password

Credentials

(Let us know how you want to receive them)

Thank you