## Project Plan

- Cryptography: A dynamic and vibrant field in theoretical computer science
- Create an online encyclopedia for theoretical cryptography
- To present all the content in one place in a lucid way
- A tutorial for first-time learners and a reference for experts/researchers

## Salient Features

A hybrid between a textbook and the Wikipedia

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start from basics, go in-depth</td>
<td>Open access. Shows up on Google.</td>
</tr>
<tr>
<td>Reliable information</td>
<td>Dynamic/frequently updated content</td>
</tr>
<tr>
<td>Coherent presentation</td>
<td>Easy browsing, with cross-references</td>
</tr>
<tr>
<td>Compilation of important results</td>
<td>Multiple views (by lectures, categories..)</td>
</tr>
<tr>
<td></td>
<td>Multiple contributors</td>
</tr>
</tbody>
</table>

## Work Done This Summer

Read extensively and added sections on

- Zero Knowledge Proofs
  - Protocol for Alice to convince Bob that she knows a secret without letting Bob learn anything about it except what he already knows
  - Used for enforcing honest behavior in cryptographic protocols
  - Numerous variants/issues

- Commitment Schemes
  - Alice puts a piece of information in a locked box and gives it to Bob, while retaining the key. Later she can reveal the information by giving the key to Bob

## Remaining Work

- A proper bibliography needed.