ISEC 601 - Group 03 - Teaching Aide Walkthrough

By Azeezat Lawal, Dami Ogunnupebi, Pradip Ghimire, Abdul Osuwa and Tarun Sidhu

Hi there!

Do you like humorous comics?
Are you interested in learning about some crypto-graphic methods that allow data to be shared, without revealing sensitive information to unauthorized parties?
If your answer to these two questions are yes, and I bet it is, well I have just the right teaching aide for you!

This is a self-paced teaching aide that has all the information that you need, on privacy preserving cryptography. Privacy Preserving Cryptography is the crypto-graphic method that allows data to be shared and processed without revealing sensitive information to other unauthorized parties. The techniques of this crypto-graphic method that we will teach include:

- Zero-Knowledge Proofs,
- Homomorphic Encryption,
- Secure Multi-Party Computation,
- Differential Privacy, and finally,
- Anonymous Credentials and Commitment Schemes

We know that learning something new can be tough, so we have prepared a brand new, easy to follow, teaching aide to educate you on privacy preserving cryptography methods.

We also know that learning something new can be very boring, so we included some comics explaining the methods. These comics are inspired by xkcd, and we have dubbed ours “xkcdon’t” and “xkcdo”, to show you what to do and what not to do for each technique.

These comics are made of easy-to-follow real life scenarios so that just when your eyes are about to glaze over, they wake you right up, and hopefully make you laugh (either because they are really funny or just so bad that you can’t help but laugh).

Finally, our teaching aide includes a longer supplementary document with information we’ve gathered on the methods for further reading below, just in case you want to learn more about Privacy Preserving Cryptography.

Happy learning!