CPE 593- Applied Data Structure & Algorithms

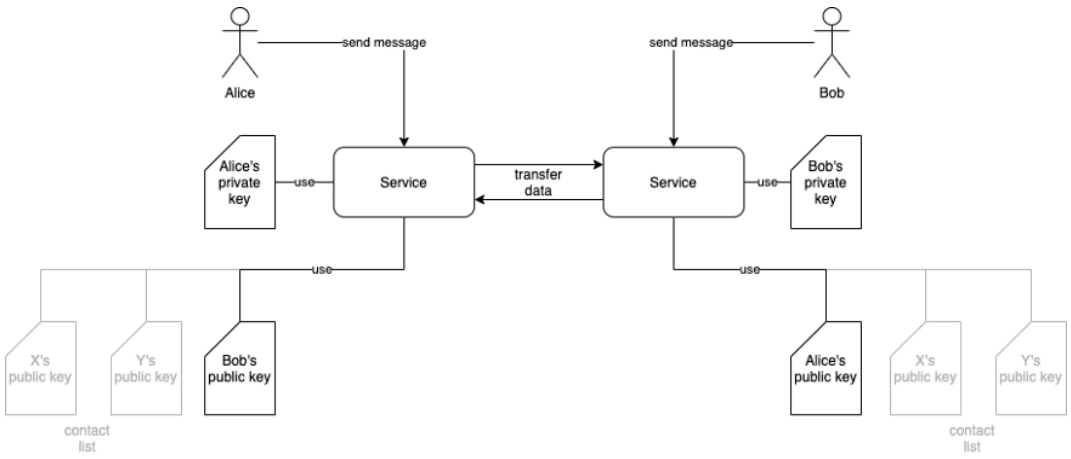
Group Members: Amanda Ly, Ghaith Arar, Neel Haria

Language: C++

Topic: Implement RSA using a biginteger library. It doesn't have to be production quality, but you would need to implement Diffie-Hellman key exchange and use AES-256 (you don't have to write that) to exchange secret messages.

GitHub: CPE-593_FinalProject-RSA

Abstract: RSA is perhaps the most widely used encryption public- key (PK) cryptography. There is a high probability that this document was delivered to the reader, at some point, using this algorithm. However, for any cryptography scheme, security is the main incentive. To implement a secure RSA scheme very large prime numbers are required; therefore, the algorithm is computationally intensive. This project will look into various implementations of the RSA algorithms, then it will implement the RSA in an efficient and elegant fashion using C++. The implementation will not only try to implement secure algorithms, but it will also find a very efficient implementation.



Brief Background on RSA:

Under RSA encryption, messages are encrypted with a public key and can only be decrypted by the private key. Each RSA user has a key pair consisting of their public and private keys. RSA encryption is often used in combination with other encryption schemes, or for digital signatures which can prove the authenticity and integrity of a message. It isn't generally used to encrypt entire messages or files, because it is less efficient and more resource-heavy than symmetric-key encryption. To make things more efficient, a file will generally be encrypted with a symmetric-key algorithm, and then the symmetric key will be encrypted with RSA encryption. Under this process, only an entity that has access to the RSA private key will be able to decrypt the symmetric key.

Aspects of RSA Encryption:

- Trapdoor functions: makes it easy to compute in one direction but incredibly hard to reverse
- Generating primes: allows PKs to be shared without endangering the message or revealing the private key
- Carmichael's totient function: used to generate public and private key

Overall Tasks: (tasks are subject to change)

- **Everyone:** paper & presentation
- **Amanda: for text**
  - Public/private key generation
  - Message encryption
- **Neel: for text**
  - Message decryption
- **Ghaith:**
  - Diffie-Hellman Key Exchange

References (In Overleaf Format):


```
% Cite1
@book{kahate2013cryptography,
  title={Cryptography and network security},
  author={Kahate, Atul},
  year={2013},
  publisher={Tata McGraw-Hill Education}
}

% Cite2
@misc{contributors_2020,
 title={What is asymmetric cryptography and how does it work?},
 author={Brush, Kate and Rosencrance, Linda and Cobb, Michael},
 year={2020},
 url={https://searchsecurity.techtarget.com/definition/asymmetric-cryptography},
 journal={SearchSecurity},
 publisher={TechTarget}}

% Cite3
@article{rivest1978method,
  title={A method for obtaining digital signatures and public-key cryptosystems},
  author={Rivest, Ronald L and Shamir, Adi and Adleman, Leonard},
  journal={Communications of the ACM},
  volume={21},
  number={2},
  pages={120--126},
  year={1978},
  publisher={ACM New York, NY, USA}
}

% Cite4
@inproceedings{zhou2011research,
  title={Research and implementation of RSA algorithm for encryption and decryption},
  author={Zhou, Xin and Tang, Xiaofei},
  booktitle={Proceedings of 2011 6th international forum on strategic technology},
  volume={2},
```

pages={1118--1121},
year={2011},
organization={IEEE}
}

% Cite5
@article{carts2001review,
title={A review of the Diffie-Hellman algorithm and its use in secure internet protocols},
author={Carts, David A},
journal={SANS institute},
pages={1--7},
year={2001}
}

% Cite6
@article{diffie1976new,
title={New directions in cryptography},
author={Diffie, Whitfield and Hellman, Martin},
journal={IEEE transactions on Information Theory},
volume={22},
number={6},
pages={644--654},
year={1976},
publisher={IEEE}
}

% Cite7
@article{kallam2015diffie,
title={Diffie-hellman: Key exchange and public key cryptosystems},
author={Kallam, Sivanagaswathi},
journal={Master degree of Science, Math and Computer Science, Department of India State University, USA},
pages={5--6},
year={2015}
}

% Cite8
@article{raymond2000security,
title={Security issues in the Diffie-Hellman key agreement protocol},
author={Raymond, Jean-Fransico and Stiglic, Anton},
journal={IEEE Transactions on Information Theory},
volume={22},
pages={1--17},
year={2000},
publisher={Citeseer}
}

Coding References:

Cite 1: https://www.tutorialspoint.com/cplusplus-program-to-implement-the-rsa-algorithm

Cite 2: https://stackoverflow.com/questions/7560114/random-number-c-in-some-range