Project #1

Graded

Student

Kevin Vuong

View or edit group

Total Points

93 / 100 pts

Question 1

Written

38 / 40 pts

– **0 pts** Good Job!

– **1 pt** Missing some in-text citations

– **3 pts** Missing all in-text citations

– **1 pt** References missing access dates

– **1 pt** Some grammatical issues

– **1 pt** Some issues with References

✔ – **2 pts** Missing conclusion

– **1 pt** Paper lacks logical flow

– **1 pt** Some incorrect information

I already graded your partner's work. Please see that for comments, and do NOT upload more than one per group.

Question 2

Gram-Schmidt (link)

28 / 30 pts

- **– 0 pts** Correct. Nice job!
- **– 2 pts** What about n vectors in $\mathbb{R}^m$?
- ✔ **– 1 pt** orthogonalized, not orthonormalize
- **– 1 pt** What if the vectors are linearly dependent?
- **– 2 pts** missing comments
- **– 1 pt** does not properly convert string to float
- **– 5 pts** only works for a particular shape matrix
- **– 10 pts** returns incorrect calculations
- ✔ **– 1 pt** input rows, output columns
- we want floating point arithmetic

Question 3

RSA (link)

27 / 30 pts

- **– 0 pts** Correct
- ✔ **– 1 pt** p and q need to be distinct
- **– 1 pt** What if p and q are not prime?
- **– 2 pts** Missing comments
- **– 3 pts** missing or incomplete key generation function
- **– 3 pts** missing or incomplete encryption function
- **– 3 pts** missing or incomplete decryption function
- **– 2 pts** need instructions for user (i.e. $m < n$)
- **– 2 pts** functions not taking correct input
- **– 3 pts** missing print statements
- **– 1 pt** What if $m > n$?
- **– 1 pt** $m \neq 0$
- ✔ **– 2 pts** missing some output/print statements

No questions assigned to the following page.

Kevin Vuong & Andrew Brooks

Prof. Acitelli

ACMS 40100 Intro to Mathematical Cryptography with Python

February 19 2024

(Gram-Schmidt Orthonormalizer Algorithm & RSA Encryption Implementation)

"We stand today on the brink of a revolution in cryptography" wrote Whitefield Diffie and Martin Hellman in their famous 1976 paper 'New Directions in Cryptography.' And they certainly were not wrong. With this paper, they introduced the idea of Public Key Cryptography, a novel cryptosystem that transformed the landscape of cryptography and ensured the security of telecommunications and the internet (Cloudflare 1).

Public Key Cryptography generally consists of users in a community, where each user has a certain pair of keys known as a public and private key. The public key is distributed by each user into a publicly available "ledger" while the private key is kept secret by the user. Together, these pairs of keys allow any user to send and receive data from another individual and only that individual, even if they've never met or performed any previous transfers of data (IBM 1). Cryptosystems also provide a list of other requirements, and can be summarized as follows: Integrity, which signals whether the data was altered at all; Authentication, which confirms a message was sent from the actual sender; Non-repudiation, which means the sender cannot deny the authenticity of their signature (i.e. rescind their signature.) And confidentiality, which ensures that the data hasn't been accessed by a third party (Acitelli 1).

No questions assigned to the following page.

How Public Key Cryptography satisfies these requirements, and especially the last requirement of confidentiality, is incredibly important to the integrity of the cryptosystem. Public Key Cryptography achieves these requirements by using the idea of a 'one-way function,' also known as a 'trapdoor-function' (Vadhan 1). A one-way function is any function in which f is easy to calculate, but f^{-1} is (or at least believed to be) far more difficult (or impossible) to calculate computationally. If the user maintains the secrecy of f^{-1} and scales up the computational complexity of computing f^{-1} to an unreasonable amount, then only the user knows f^{-1}, which allows anyone to send data to the user by first wrapping it in f (Diffie and Hellman 654). By creating this function, the user also implicitly satisfies the other requirements, but it will not be discussed how in this paper.

As Diffie and Hellman put it, "secrecy is the most important part of cryptosystems" (Diffie and Hellman 654). However, public key cryptography differs from previous types of cryptography in what exactly is kept secret. For example, the Caesar cipher (where letters in a word are replaced by a letter three places down in the alphabet), depends on keeping the entire encryption process a secret. Additionally, systems were limited to calculations that could be done by hand or devices such as the enigma machine. These types of cryptosystems could be cracked by a thief stealing a machine or learning the encryption process. Public key cryptography, however, is a novel idea in that the system for encryption is public knowledge. This was a completely revolutionary idea that defied previous thought; experts thought that a public algorithm would compromise the security of a cryptosystem (Diffie and Hellman 654). Yet, this turned out to be the idea that would ensure a superior cryptosystem. Furthermore,

No questions assigned to the following page.

algorithms for encrypting and decrypting can be carried out by computers, and modern mathematical theories can determine the computational complexity of cracking these systems (Diffie and Hellman 654). This ensures that public key cryptography is more desirable and secure than previous methods.

RSA is overwhelmingly the most popular public key cryptosystem used today. The Secure Sockets Layer (SSL) protocol, for example, is a common use of RSA used by web browsers to ensure secure transactions online. Webpages equipped with SSL have addresses that begin with “https” while webpages without SSL begin with “http” (Koblitz and Menezes 607). The server of a secure webpage transmits a certificate to the client, including identifying information and a public key. The client creates a random session key, encrypts the cipher message, and transmits the result to the server. Overall, this system allows for secure transactions that occur daily online.

Unlike RSA, knapsack cryptosystems–involving the NP-hard general knapsack problem–remain unpopular today since simple versions of the cryptosystems have been proven to crack (Koblitz and Menezes 609). The Digital Signature Algorithm (DSA), created by the U.S. National Institute of Standards and Technology in 1991, is based on the discrete log problem. This system was incredibly popular due to its high security, low implementation time, and low signature storage (Koblitz and Menezes 611). However, the elliptic curve digital signature algorithm (ECDSA) has superseded the DSA. In fact, elliptic curve cryptosystems are commonly used today for cryptocurrencies such as Bitcoin. Other popular uses of cryptosystems include providing businesses with a way to authenticate digital signatures, or for the government to transmit top-secret information (Hellman 46). Together, these uses of encryption justify the continued research in the

No questions assigned to the following page.

field to ensure that personal information is kept private, and top-secret information is kept out of the wrong hands.

No questions assigned to the following page.

Works Cited

Acitelli, Catie. “RSA Cryptosystem.” ACMS 40100, 2 Feb. 2024, University of Notre Dame. Class lecture.

Diffie, Whitfield, and Hellman, Martin. “New Directions in Cryptography.” *IEEE Transactions on Information Theory*, vol. 22, no. 6, IEEE, Nov. 1976, pp. 644-654. https://www-ee.stanford.edu/~hellman/publications/24.pdf.

Hellman, Martin. “An Overview of Public Key Cryptography.” *IEEE Communications Magazine,* 50th Anniversary Commemorative Issue, IEEE, May 2002, pp. 42-49. https://netlab.ulusofona.pt/im/teoricas/OverviewPublicKeyCryptography.pdf.

“How Does Public Key Encryption Work?.” *Cloudflare*, 2024. www.cloudflare.com/learning/ssl/how-does-public-key-encryption-work/.

Koblitz, Neal, and Menezes, Alfred. “A Survey of Public-Key Cryptosystems.” *SIAM Review*, vol. 46, no. 4, Society for Industrial and Applied Mathematics, 2004, pp. 599-634. https://epubs.siam.org/doi/10.1137/S0036144503439190.

“Public Key Cryptography.” *IBM*, 8 Mar. 2021. www.ibm.com/docs/en/ztpf/1.1.0.15?topic=concepts-public-key-cryptography. Accessed 20 Feb. 2024.

Vadhan, Salil. “One-Way Functions” CS 127/CSCI E-127: Introduction to Cryptography, 2013, Harvard University. Class lecture. https://people.seas.harvard.edu/~salil/cs127/fall13/lec7.pdf.