分組名單（不足 5 個人空著就好）:

| 姓名 | 學號 |
|---|---|
| 林幼馨 | 112550021 |
| 陳芝瑄 | 112550024 |
| 曾士珍 | 113550090 |
| 蘇宜盈 | 112550173 |
| 楊睿軒 | 112704039 |

## 1. Name of the paper

Diffie, W., & Hellman, M. (2021). New Directions in cryptography (1976).

## 2. Summary

This paper explores innovative approaches to public key cryptography and the associated challenges. It emphasizes the need for secure communication over public channels without the requirement of a pre-shared secret key. The paper introduces the concepts of public key distribution systems and digital signatures to address privacy and authentication issues in teleprocessing systems. It also delves into computational complexity as a means to ensure the security of cryptographic systems, contrasting this with unconditionally secure systems like the one-time pad.

## 3. Strength(s) of the paper

- **Innovative Concepts**

  The paper presents groundbreaking ideas such as public key cryptography and digital signatures, which form the foundation of modern cryptographic practices.

- **Addressing Practical Challenges**

  It effectively addresses real-world problems in key distribution and authentication, making it highly relevant for contemporary business communications and secure digital interactions.

- **Theoretical Contributions**

  The authors link cryptographic security with computational complexity, providing a solid theoretical framework for future research and development in cryptography.

## 4. Weakness(es) of the paper

- **Incomplete Solutions**

  While the paper proposes several novel techniques, it acknowledges that many of the proposed solutions are partial and the problem of public key

distribution remains largely open.

- **Practical Implementation**

  The practical implementation details and performance considerations of the proposed cryptographic systems are not thoroughly explored, leaving room for further research and experimentation.

- **Complexity Assumptions**

  The reliance on computational complexity as a measure of security, though innovative, assumes that current computational hardness assumptions (like factoring large integers) will hold true, which may not account for future advances in computing, such as quantum computing.

## 5. Reflection

### ➢ What did you learn from this paper?

This paper detailly mentioned the transformation of cryptography from an art to a science, which is mainly driven by theoretical advancements in information theory and computer science. It also highlights the practical applications of these new cryptographic methods in securing digital communications and transactions. The following are some key insights:

1. **One-Way Functions**

   In the article, it discussed the importance of one-way functions in cryptography. These functions are easy to compute in one direction but difficult to reverse, making them suitable for creating secure cryptographic systems. Otherwise, it may easily be decrypted.

2. **Public Key Cryptography**

   Diffie and Hellman introduce the concept of public key cryptography. Before, a shared secret key is required to allow secure communication. However, with the introduction of public key cryptography, secure communication without the need for a shared secret key distributed via a secure channel is realized. This innovation addresses the major challenge of key distribution in cryptography. It makes secure communication much easier to complete. Not requiring a secure channel for distributing a shared secret key also cost down and simple the process. Public key cryptography fundamentally changes how secure communications are established. Each user can publish their public key in a directory, allowing any other user to send encrypted messages that only the intended recipient can decrypt. This breakthrough addresses the major barrier to the adoption of teleprocessing networks for business communications, where the delay

and cost of traditional key distribution methods are impractical.

3. **Revolution in Cryptography**

   In the paper, the author mentioned significant improvement in cryptography made possible by the advancements in computer hardware. It lowered the costs of cryptographic devices, and therefore makes it more accessible for commercial applications such as remote cash dispensers and computer terminals. The hardware advancements lead to a departure from the era when cryptographic devices were mechanical and costly, which restricted their use to military and governmental applications. The widespread availability of cheap digital hardware has democratized access to cryptographic technologies, paving the way for their integration into everyday commercial transactions.

4. **Digital Signatures**

   In the paper, the author proposes the use of digital signatures, which provide an equivalent of a written signature in electronic communications. This is crucial for verifying the authenticity of digital messages and ensuring non-repudiation in electronic transactions. Digital signatures play a crucial role in various applications, from securing email communications to validating software updates. They ensure that a message has not been tampered with and confirm the identity of the sender, addressing the challenge of authentication in electronic communications. Digital signatures serve as a cornerstone in establishing trust and integrity in digital interactions, offering robust security measures against unauthorized access and fraudulent activities.

5. **Cryptographic Challenges and Solutions**

   In the paper, the author also mentioned some major problems in cryptography we used to have, including the secure key distribution and authentication. It explained that how public key distribution systems and one-way authentication systems may provide solutions to these challenges. The traditional approach to key distribution involves transmitting keys over a secure channel, which is impractical for many applications. The paper proposes two innovative approaches to this problem: public key cryptosystems and public key distribution systems. In a public key cryptosystem, each user has a pair of keys, one public and one private. The public key is used to encrypt messages, while the private key is used to decrypt them. This system allows secure communication without the need for a pre-shared secret key, making it

ideal for applications where users have no prior relationship. Public key distribution systems take a different approach by allowing users to exchange keying information over an insecure channel in a way that makes it computationally infeasible for an eavesdropper to derive the key. This approach leverages the concept of one-way functions and other cryptographic techniques to ensure the security of the key exchange process.

6. **Authentication**

   Authentication is also a critical challenge mentioned in this paper. In traditional business communications, the signatures on a physical document provide a means of verifying the authenticity of a message. However, in the digital communication, a different approach is needed, as physical signature are not possible. Diffie and Hellman propose the use of cryptographic techniques to provide message authentication, ensuring that a message has not been altered and verifying the identity of the sender. The paper discusses the concept of one-way authentication, where a message's authenticity can be verified without revealing the secret key used to generate it. This is crucial for applications where the integrity and authenticity of a message must be assured, such as in financial transactions and secure communications.

- **How would you improve or extend the work if you were the author?**

1. **Integration with Modern Cryptographic Algorithms**

   The paper discusses foundational concepts in cryptography, such as public key cryptography and digital signatures. Incorporating modern advancements such as elliptic curve cryptography (ECC) is considerable. ECC offers similar levels of security with smaller key sizes compared to RSA, making it more efficient and suitable for contemporary applications.

2. **Quantum-Resistant Cryptography**

   With the advent of quantum computing, many existing cryptographic systems could become vulnerable. Extending the paper to explore quantum-resistant algorithms, such as lattice-based cryptography, would provide a future-proof solution against the threats posed by quantum computers.

3. **Real-World Implementation and Performance Metrics**

   To enhance the practical relevance, we can add detailed case studies and

performance metrics from real-world implementations. This could include benchmarks of cryptographic systems in different environments, such as cloud computing or IoT devices.

4. **User-Friendly Cryptographic Applications**
   Extensions includes designing intuitive interfaces and protocols that ensure strong security while being easy to use for non-technical users could also be valuable.

## ➢ What are the unsolved questions that you want to investigate?

1. **Scalability of Cryptographic Protocols**
   With billions of devices communicating simultaneously, cryptographic protocols must be optimized to handle the massive scale of the internet. Investigating scalable solutions for key management and encryption would be crucial.
2. **Post-Quantum Cryptography**
   We can develop and standardize quantum-resistant cryptographic methods by finding the most effective cryptographic algorithms that can resist quantum attacks and how can they be efficiently implemented in existing systems.
3. **Side-Channel Attacks and Mitigations**
   In order to protect cryptographic implementations against side-channel attacks which exploit physical leakage such as power consumption or electromagnetic emissions. Researching robust countermeasures to these types of attacks is essential for the security of cryptographic devices.
4. **Privacy-Preserving Cryptographic Techniques**
   Developing cryptographic techniques that not only secure data but also preserve user privacy is important. This includes investigating homomorphic encryption, which allows computations on encrypted data without decrypting it, thus ensuring data privacy even in processing.

## ➢ What are the broader impacts of this proposed technology?

This paper covers advancements in cryptography and computational complexity theory, both of which have had significant and wide-ranging impacts across various fields.

1. **Commercial Activities**
   Advances in encryption systems have revolutionized commercial activities, facilitating secure electronic commerce and digital

transactions. Authentication mechanisms ensure that only authorized users can perform operations, allowing for safe financial transactions online. These advancements have bolstered consumer trust in online transactions, fostering economic growth and innovation.

2. **Online Platforms**

   These advancements have made network communication more secure, preventing unauthorized third parties from intercepting and stealing sensitive information, which ensuring data integrity and confidentiality. This has led to widespread adoption across sectors such as social media, e-commerce, and healthcare.

3. **Regulatory Compliance**

   Cryptographic techniques play a crucial role in ensuring compliance with data protection regulations such as GDPR and HIPAA. By implementing encryption and digital signature technologies, organizations can protect sensitive data, mitigate the risks of regulatory non-compliance, and build trust among users and stakeholders.

4. **Technological Innovation**

   Research in computational complexity theory has driven innovations in algorithm design and optimization, leading to advances in fields such as artificial intelligence, machine learning, and quantum computing. Understanding the computational difficulty of problems has enabled the development of more efficient algorithms and computing techniques, thereby enhancing technological capabilities.

5. **Personal Empowerment and Digital Autonomy**

   The widespread application of cryptographic technologies has empowered individuals to better control their digital identities and personal information. By utilizing encryption and digital signatures, users can protect their privacy and assert their digital autonomy in an increasingly connected world.

## ➢ Current Development of Diffie-Hellman key exchange

The Diffie-Hellman key exchange is a cryptographic protocol which is widely applied and has evolved to address modern security challenges.

1. **Larger Prime Modulus:**

   the original Diffie-Hellman protocol employed prime modulus of relatively small sizes, a characteristic that has since been upgraded to employ primes of at least 2048 bits, a significant enhancement for bolstering security measures.

2. **Elliptic Curve Diffie-Hellman (ECDH):**
   Uses elliptic curve cryptography for better security with shorter key lengths and higher efficiency, suitable for resource-constrained devices.
3. **Ephemeral Diffie-Hellman (DHE or ECDHE):**
   Generates temporary key pairs for each session, providing forward secrecy to secure past session data even if long-term keys are compromised.
4. **Secure Parameter Generation:**
   Emphasizes robust security parameters, such as high-quality random number generators and verified prime generation processes to avoid mathematical weaknesses.
5. **Hybrid Key Exchange Methods:**
   Combines Diffie-Hellman with other encryption methods (e.g., TLS 1.3 using ECDHE and RSA) to enhance overall security and performance.

While the original Diffie-Hellman protocol remains fundamentally secure, advancements have addressed potential vulnerabilities and adapted to modern computational capabilities, ensuring reliable security in various digital communication contexts.

## ➢ Realization of a technical specification or algorithm as a program

According to the content of the document, we can implement a simple application based on the Diffie-Hellman key exchange (DHKE) protocol. This protocol allows two untrusted parties to securely share a key over an insecure channel, which can be used for subsequent encrypted communication.

1. **Function explanation**
   - **Key Generation:** Each user generates a private key and a corresponding public key.
   - **Public Key Exchange:** Users exchange public keys and compute the shared key.
   - **Encrypt Message:** The shared key is used to encrypt messages.
   - **Decrypt Message:** The shared key is used to decrypt messages.
2. **Warning Mechanism**
   - The validate_inputs function checks whether the input values for q and alpha are valid. If q is not prime or alpha is not within the range 1 to q, it raises a ValueError.
   - In the main function, user input prompts for q and alpha. If the

input values are not valid, the ValueError raised by validate_inputs is caught, and an appropriate error message is displayed.

3. **Customization**
   - You can change the prime number q and the primitive root alpha in the main function to experiment with different values.
   - The encryption and decryption algorithms can be modified to suit different application needs.
4. **Sample Output**

   When running the script with valid inputs, you will see prompts to input a prime number and a primitive root. The script will then output something similar to the following:

```
Please input a prime number q: 173
Please input a primitive root alpha: 5
User A's private key: 159
User A's public key: 166

User B's private key: 145
User B's public key: 79

User A's shared key: 102
User B's shared key: 102

Key exchange successful! Both users have the same shared key.
```

```
Original message: Hello, this is a secret message.
Encrypted message: bytearray(b'\x7f\xe6#CJZ\x0fW\x89\x9e9su\xcdd
    <\x97N\x02\x06\x99\x83|X\xca\xba\xcd\xbe\x1c-\x93\xcf')
Decrypted message: Hello, this is a secret message.
----
Original message: Short msg
Encrypted message: bytearray(b'd\xeb ]QVBP\x86')
Decrypted message: Short msg
----
Original message: This message is longer than the others and should
    still be encrypted correctly.
Encrypted message: bytearray(b'c\xeb&\\\x05\x1bJP\x92\x96-6
    <\xd77}\xdbR\t\x02\x8e\x94
    (\x0c\xcf\xbe\xd0\xed\t"\x93\xc1X\xf7\'JW\x05\x0fB\x8f\x93j
    t\xd111\xd3\x1d\x14\x11\x82\x8adX\xc5\xba\x9e\xa8\x13
    )\x84\x98G\xf7*K\x05\x15@Q\x93\x92)\'p\xc7j')
Decrypted message: This message is longer than the others and should
    still be encrypted correctly.
----
```