PROJECT - Science, Technology and Society

Topic : Critical analysis on “Cryptography” as a Technology using STS concepts.

- By Aishani Pandey (2022121009) , Ayush Maurya (2021115004) , Harshvardhan(2021111017)

1. Introduction

1.1. Overview of Cryptography

Cryptography is the practice of secure communication, which has developed from its historical foundations to become essential in today's digital environment. In order to safeguard data and make sure that only the intended receivers can read it, codes and algorithms must be created. Early instances of cryptography can be discovered in ancient Greece and Egypt, whose history extends back thousands of years. These days, it involves sophisticated procedures, intricate mathematical calculations, and cutting-edge technology that safeguard authenticity, secrecy, and integrity of data.

1.2. Importance of Cryptography

Cryptography is essential in our networked world to secure online transactions, protect private data, and preserve individual privacy. Applications of Cryptography include digital signatures, online banking, private messaging, and secure military communications. The cornerstone of information security, cryptography is crucial in the digital age as it guards against illegal access, cyberattacks, and data breaches.

1.3. Purpose of Analysis

Through the use of the frameworks studied in the "Science, Technology, and Society" course, this study seeks to critically analyze cryptography. The report will analyze how cryptography influences and is influenced by sociological, cultural, and political variables by looking at it from viewpoints such as the Social Construction of Technology (SCOT), Actor-Network Theory (ANT), and Technological Determinism. The historical evolution of cryptography, its social effects, and the moral, political, and financial ramifications of its application will all be included in the analysis.

2. Historical Context and Development

2.1. Ancient Roots

Ancient cryptography began with many methods to conceal information by early civilisations, including the Egyptians, Greeks, and Romans. Among the well-known examples is the 400 BC military communications between the Spartans and the scytale transposition cipher. The parchment strip had to be wrapped around another baton of the same proportions to decipher a message that had been jumbled. The Kama Sutra claims that a kind of cryptography known as Mlecchita vikalpa was employed in India for secret love letters between 400 BC and 200 AD. Furthermore, Julius Caesar is credited for using the Caesar cipher, a replacement cipher in which the ciphertext was produced by moving each character in the plaintext by three places.

2.2. Evolution and Advancement

Over the history of cryptography, both the development of encryption techniques and the countermeasures employed by cryptanalysts to get past them have improved dramatically. Especially in the pre-20th century, this era was characterised by the employment of manual procedures and the continuous game of cat and mouse between cryptographers and cryptanalysts.

Classical cryptography primarily used human techniques for message encrypting and decoding before computers were widely used. Among these were substitution, transposition, and polyalphabetic ciphers. Demand for safer communication methods led to developing ever more complex ciphers, including the Vigenère

encryption. As cryptanalysts found methods to break simpler ciphers, cryptographers created increasingly intricate encryption algorithms.

2.3. 20th century and Modern Era

The development of computers and the increasing need for secure communication during the 20th and current centuries have caused a significant revolution in cryptography, initially driven for military use and then for modern communication.

Cryptography played a significant role in both World Wars; the infamous Enigma machine is just one example. The complex electromechanical Enigma machine was built by German soldiers and used a series of rotors to encrypt communications.

Because of its complexity, which made breaking it very difficult, Germany extensively used the machine during World War II. Ultimately, though, Polish cryptographers who shared their findings with the British and French intelligence services as well as Alan Turing and his colleagues at Bletchley Park's groundbreaking work allowed Enigma-encrypted communications to be successfully decoded. Turing's creation of the Bombe machine—a tool for deciphering the Enigma code—helped the Allies win World War II.

When computers were invented in the 20th century, cryptography underwent a revolution. Higher order mathematical operations and data storage capacities enabled the development of advanced encryption methods and algorithms.

Creation of public-key cryptography in the 1970s was one of the biggest developments in contemporary cryptography. With this asymmetric cryptography approach, information could be sent securely without requiring a shared secret key. From conventional symmetric-key cryptography, which needed the sender and recipient to have the same key, this was a major change.

Best represented by algorithms like RSA, public-key cryptography allowed for safe online transactions and communication while safeguarding private information, so enabling cryptography to be widely used in the digital era.

Cryptography is essential for protecting many parts of our lives in the digital era, including safe messaging, data storage, and online banking. Ever more reliable cryptographic algorithms and methods have to be developed due to the growing dependence on digital communication and ongoing technical breakthroughs. As

computing power increases, cryptographers are always trying to thwart possible attacks including brute-force and quantum computing-based ones. One example of the continuous work to future-proof cryptographic systems—that is, to develop encryption techniques that can resist the power of quantum computing—is the development of post-quantum cryptography.

The development of cryptography in the 20th century and the present has been influenced by its critical role in both World Wars, the introduction of computers and public-key cryptography, the emergence of contemporary cryptography, and the growing significance of cryptography in the digital age and beyond.

2.4. Cryptoanalysis as a counterpart

Mathematicians and codebreakers have worked with cryptographers throughout history to crack ciphers currently in use. Cryptanalysis is a crucial complementary method to cryptography, deciphering encrypted messages without the decryption key. In reaction to developments in cryptanalysis, more complicated ciphers have often been developed.

Cryptologists have cracked ciphers by many techniques, including:

By counting the number of times each letter appears in the ciphertext, frequency analysis searches for trends and potential keys. Cryptologists may deduce the substitutions in a monoalphabetic substitution cipher from their knowledge of the plaintext letter frequency distribution.

Krasinski Analysis With a polyalphabetic cipher, such as the Vigenère cipher, this approach searches the ciphertext for recurrent patterns to ascertain the length of the key. Cryptanalysts can use the interval between successive ciphertext sequences to determine the keyword's size.

The Friedman Test compares the frequency of letters in the plaintext to that of the ciphertext to search for potential keys. Using the Friedman test, one may determine how many alphabets a polyalphabetic cipher will likely use.

3. Theoretical Frameworks

3.1. Social Construction of Technology

The Social Construction of Technology (SCOT) framework views technology as a social product shaped by the interpretations and interests of various social groups. It provides a valuable lens to examine how different actors have influenced the development and use of cryptography.

3.1.1. Interpretative Flexibility

Interpretative flexibility refers to the notion that different social groups can have different interpretations and uses of a technology. In the context of cryptography, this concept is particularly relevant due to the varied perspectives on its purpose and application.

1) **Military Use:**

- The military and defense sectors view cryptography as a strategic tool for secure communication.
- They emphasize the need for robust encryption to safeguard sensitive information and maintain national security.
- Military cryptography focuses on creating and maintaining unbreakable codes, often for secure communication during warfare or in intelligence operations

2) **Civil Use:**

- Civilians and civil society organizations view cryptography as a means of protecting their personal data, maintaining privacy, and establishing secure digital communication.
- Civil use emphasizes individual freedom, protecting sensitive information in online transactions, and ensuring secure personal communication

3) **Commercial Use:**

- Businesses utilize cryptography to secure digital transactions, protect customer data, and safeguard proprietary information.
- The commercial perspective focuses on building trust in e-commerce and digital services, emphasizing strong encryption to prevent data breaches and protect intellectual property

However , there were varied uses and interpretations of cryptography that can lead to conflicts among different social groups.

Conflict of Interpretations:

1) **Government Perspective:**

- Governments often view strong encryption as a potential hindrance to law enforcement and national security efforts.
- They may advocate for backdoors or weakened encryption to access encrypted communications during criminal investigations or counter-terrorism operations

2) **Privacy Advocate Perspective:**

- Strong encryption is seen by privacy advocates as necessary to safeguard individual liberties and stop illegal access to personal information.
- They claim that government attempts to weaken encryption or create backdoors violate people's right to privacy and civil freedoms, hence they are against them.

3) **Business Perspective:**

- Businesses typically support strong encryption to protect their data and ensure secure digital transactions.
- They may be concerned about regulatory burdens or government access requirements that could compromise their proprietary information or customer trust

Case Study - Apple vs. FBI:

- ❖ The conflict of interpretations was evident in the Apple vs. FBI dispute, where the government sought access to encrypted communications for security reasons.
- ❖ Apple defended the right to strong encryption, arguing that creating a backdoor would compromise the security and privacy of all its users.

3.1.2. Relevant Social Groups

SCOT highlights the importance of relevant social groups, which influence and interpret technologies based on their interests and needs.

1) **Governments:**

- Governments have a vested interest in cryptography for national security reasons but also face challenges when encryption hinders law enforcement or surveillance efforts.
- The government's stance on cryptography often balances between ensuring security and addressing concerns over privacy and civil liberties.

2) **Hackers:**

    - Hackers can be both adversaries and innovators in cryptography.
    - They exploit weaknesses in encryption for malicious purposes but also contribute to the development of more robust cryptographic methods.

3) **Businesses:**

    - Businesses use cryptography to secure transactions, protect customer data, and safeguard proprietary information.
    - Their interests align with strong encryption but may also be concerned about regulatory burdens or legal requirements for access.

4) **Privacy Advocates:**

- Privacy advocates champion the use of cryptography to protect individual freedoms and prevent unauthorized access to personal data.
- They often oppose government attempts to weaken encryption or introduce backdoors.

3.1.3. Technological Frames

Technological frames represent the shared assumptions, practices, and expectations that shape how a technology is understood and used.

1) **Societal Forces:**

- Social forces, such as privacy concerns, regulatory requirements, and the demand for secure communication, have significantly influenced the evolution of cryptographic technologies.
- Public controversies, like the Apple vs. FBI case, highlight societal debates over encryption

2) **National Security Frame:**

- The national security frame focuses on cryptography's role in safeguarding national interests and preventing cyber threats.
- This frame often justifies government backdoors or weakened encryption for national security purposes.

3) **Privacy Frame:**

- The privacy frame emphasizes the importance of protecting personal data and privacy rights through strong encryption.
- It argues against government access to encrypted communications.

4) **Commercial Frame:**

- The commercial frame views cryptography as a tool for enabling secure commerce and protecting proprietary information.
- This frame generally supports strong encryption but might have concerns about regulatory burdens.

3.1.4. Closure and Stabilization

1) **Government Regulation:**

- One form of closure might be through government regulation, where the state imposes specific encryption standards or access requirements.
- This type of closure can align with the national security frame but may face resistance from privacy advocates

2) **Industry Standards:**

- Another form of closure could come from industry standards bodies, which establish accepted encryption protocols for different applications.
- This form of closure aligns with the commercial frame and supports interoperability and secure transactions.

3.1.5. Wider Context

SCOT also considers the wider social, cultural, and political context in which technology develops.

1) **Political Influences:**

- Government policies and political agendas can heavily influence the development and use of cryptography.
- Political decisions, such as export restrictions or surveillance laws, shape the landscape of cryptographic technologies

2) **Cultural Norms:**

- Cultural attitudes towards privacy, security, and authority can affect how cryptography is perceived and used.
- Different cultures may prioritize individual freedoms or collective security, influencing their stance on encryption.

3) **Economic Factors:**

- The economic interests of businesses and industries that rely on encryption can shape its development and deployment.
- The commercial frame emphasizes the economic benefits of secure communication and proprietary protection.

3.2. Actor-Network Theory

Actor-Network Theory (ANT) is a theoretical and methodological approach to social theory that emphasizes the interconnectedness of all entities in the social and natural worlds through constantly shifting networks of relationships. In ANT, both human and non-human entities are considered "actors" that interact to form "networks." The framework is useful for analyzing cryptography because it allows us to consider the influence of both human and non-human elements in shaping this technology.

By applying ANT to cryptography, we can understand how various actors, both human and non-human, interact and align their interests within complex networks. This approach highlights the interconnected nature of technology and society and shows how cryptographic systems are not just technical artifacts but are shaped and maintained by networks of actors with diverse interests.

3.2.1. Actors And Networks:

In ANT, all entities involved in a network are considered actors, including people, technologies, organizations, and even abstract concepts. In the context of cryptography, the actors and networks include:

- **Human Actors:** These include:
  - Cryptographers
  - Government Officials
  - Hackers
  - Users
  - Organizations that develop or use cryptographic systems.

- **Non-Human Actors:** These include:
    - Cryptographic Algorithms
    - Encryption Hardware
    - Software Protocols
    - Communication Networks.

- **Networks:** The actors are interconnected to form complex networks that produce and maintain cryptographic systems. For example, a network might include a company developing encryption software, the software itself, the users, and the regulatory agencies overseeing its use.

3.2.2. Translation Processes:

Translation refers to the process by which actors align their interests to form a network. In cryptography, the key stages of translation are:

- **Problematization:** An actor (often a central or influential one) defines a problem and positions itself as an obligatory point of passage (OPP). For example, a cryptographer might define secure communication as a critical problem and position a new encryption algorithm as the solution

- **Interessement:** The central actor attempts to lock other actors into their defined roles. For example, a tech company might convince customers that their encryption software is essential for secure communication.

- **Enrolment:** The actors accept and enact the roles defined for them. For example, the users adopt the encryption software, while the government might monitor its use.

- **Mobilization**: The central actor ensures that all enrolled actors support the network's goals. For example, the tech company might lobby for favorable encryption regulations.

3.2.3. Immutable Mobiles:

Immutable mobiles are entities that maintain their form and can move across networks. In cryptography:

- **Encryption Standards**: Standardized encryption protocols are immutable mobiles because they retain their form and can be implemented in various contexts, such as in banking, communications, and data storage.

- **Cryptographic Keys:** These are unique identifiers that travel across networks to enable or restrict access to encrypted information.

3.2.4. Black Boxing:

Black boxing refers to the process by which complex networks or technologies become taken for granted and are no longer questioned. In cryptography:

- **Encryption Algorithms:** Complex cryptographic algorithms might become black boxes, where users rely on them without understanding their internal workings.

- **Secure Systems**: Systems that use encryption, like secure email or messaging apps, might be black boxed as users take their security for granted

3.2.5. Obligatory Points of Passage (OPP):

An OPP is an actor or process that all actors must go through to achieve their goals. In cryptography:

- **Certification Authorities:** These entities act as OPPs for secure digital communication, as they issue digital certificates that verify identities.

- **Encryption Libraries:** Developers might rely on specific encryption libraries as OPPs to implement secure communication in their applications

3.2.6. Controversies and Displacement:

ANT also examines controversies and displacement within networks. In cryptography:

- **Encryption Backdoors**: Controversies arise when governments demand backdoors in encryption systems, displacing the role of secure communication and leading to conflicts among actors.

- **Algorithm Shifts:** Displacement can occur when new encryption algorithms replace older ones, changing the roles and relationships within the network.

3.3. Technological Determinism

Technological Determinism is a theoretical perspective asserting that technology is the principal driving force behind societal change. According to this view, technological developments shape human behavior, culture, and institutions in a predetermined way. When applied to cryptography, this theory explores how the technology of encryption and decryption influences various aspects of society.

3.3.1. The Impact on Society:

Technological Determinism emphasizes how cryptography impacts communication, security, privacy, business, and the economy.

1) Influence on Communication:

- Encryption in Digital Communication**:** Cryptography fundamentally changes how people communicate, making digital communication more secure and private. The use of encryption in

messaging apps and email enhances confidentiality and protects sensitive information

- Impact on Transparency: While encrypted communication prevents eavesdropping, it might also limit oversight and transparency, especially in government or corporate communications. This has led to concerns about lack of accountability in secure communication channels.

2) Influence on Security and Privacy:

- Enhanced Security: Robust cryptography keeps private data safe from unwanted access, improving security for both people and businesses. Safeguarding financial transactions, personal information, and national security necessitates this.

- Privacy Protection: People can use cryptography to safeguard their personal data, which promotes a culture that respects and protects privacy. Encryption improves personal autonomy by enabling safe communication and information sharing between people.

3) Influence on Business and Economy:

- Secure Transactions: E-commerce and digital business models are enhanced by cryptography, which makes secure online transactions possible. Digital signatures, encrypted communication, and safe payment methods are essential for the digital economy.

- Competitive Advantage: By protecting client information and intellectual property, businesses that use robust encryption can achieve a competitive edge. In the digital age, consumer trust is essential for corporate success, and encryption increases it.

3.3.2. The Security vs. Privacy Debate:

The use of cryptography raises debates over the balance between security and privacy.

1) **Government Surveillance:**

- Surveillance Technologies: Governments may employ cryptography to monitor communications for the sake of national security, which may cause privacy issues. The argument used to support the push for encryption backdoors is that doing so will help fight terrorism and criminality.

- Backdoor Access: The conflict between security and privacy is brought to light by discussions about whether or not governments should have backdoor access to encrypted communications. Although governments justify access as necessary for maintaining national security, privacy activists caution that this type of access jeopardizes individual liberties.

2) **Individual Privacy:**

- Encryption for Personal Use: People are using encryption more frequently to safeguard their private correspondence and personal information, highlighting how crucial privacy is in today's world. Encryption is considered a way to secure personal information and a defense against unauthorized surveillance.

- Resistance to Surveillance: The employment of cryptography can be interpreted as a defense of individual liberties and a form of resistance against unauthorized surveillance. Conflicts between those promoting privacy and governments promoting security have resulted from this.

3.3.3. Technological Autonomy:

Technological Determinism also considers the autonomy of technology in shaping societal change.

1) **Technological Imperative:**

- Unavoidable Development: The technological imperative aspect of Technological Determinism suggests that the development and adoption of cryptography are inevitable due to its perceived benefits. This perspective views cryptographic technologies as progressing independently of societal influences .

- Technological Evolution: The progression from simple ciphers to complex encryption algorithms reflects an autonomous technological evolution, seemingly independent of societal influences. This perspective underscores the inherent drive of technology to evolve and adapt .

2) Path Dependency:

- Established Standards: Once a certain cryptographic standard is widely adopted, it becomes difficult to change, leading to a path-dependent technological trajectory. Standards like AES (Advanced Encryption Standard) have become entrenched, influencing future developments.
- Locked-In Systems: The use of specific encryption technologies in critical infrastructure can create a lock-in effect, where society is dependent on and shaped by the existing technological framework. This dependency highlights the autonomous influence of technology on societal structures .

3.3.4. Technological Influence on Human Behavior:

Technological Determinism also explores how cryptography influences human behavior and social norms.

1) Behavioral Changes:

- Communication Patterns: Cryptography changes how people communicate, encouraging secure and private exchanges over open and transparent ones. The use of encrypted messaging apps, for example, reflects a societal shift toward prioritizing privacy in communication.

- Trust and Reliability: The use of encryption fosters trust in digital interactions, influencing behavior in areas like online shopping and personal communication. Encrypted transactions provide a sense of security, which is crucial for fostering trust in digital environments.

2) **Social Norms**

- Norms of Privacy: The extensive usage of encryption upholds social norms that place a high value on individual liberty and privacy. The focus on protecting personal data is indicative of a cultural shift that values people's freedoms and rights.

- Security Awareness: As encrypted communication becomes more common, people become more conscious of the value of security and the possible dangers of exposed data. This knowledge affects how society views and behaves in relation to digital security.

3.3.5. Critiques and Limitations:

Technological Determinism faces several critiques and limitations.

1) **Overemphasis on Technology:**

    - Neglect of Human Agency: Technological Determinism's critics contend that it overemphasized technology's role while undervaluing social variables and human action. This criticism emphasizes how important it is to take into account the ways in which society and individual choices impact the advancement of technology.

    - Contextual Factors: Technological Determinism may fail to take into account the social, cultural, and political circumstances that impact the creation and uptake of cryptographic technology. This criticism highlights how crucial it is to comprehend technology in the context of a larger society.

2) **Deterministic Outlook:**

- Inflexibility: The deterministic outlook suggests a fixed path for societal change driven by technology, ignoring the potential for human intervention or alternative outcomes. This critique highlights the need for a more flexible understanding of technology's impact on society.
- Lack of Nuance: The theory might oversimplify complex interactions between technology and society, failing to capture the nuanced ways in which they influence each other. This critique underscores the importance of considering the reciprocal relationship between technology and society.

4. Critical Analysis

4.1. Ethical Considerations of Using Cryptography in Surveillance and Privacy

Along with being necessary to achieve a balance between security and privacy, cryptography raises significant ethical questions. The application of cryptography in surveillance and privacy has sparked conversations on the moral obligations of cryptographers and the social consequences of their work. The Snowden disclosures exposed the ethical dimensions of cryptography and underlined the need for a community-wide movement to oppose extensive surveillance and consider the broader consequences of cryptographic methods.

Cryptographic tool availability is a central contributor to social and economic inequality. Inequality of access to encryption technologies begs moral concerns about justice, equity, and the welfare of society. Even while encryption protects activists from repressive governments, it presents moral questions when limited to tech-savvy individuals. Moreover, the argument on how encryption affects social welfare and government openness emphasises the challenging ethical environment in which cryptographic technologies function.

4.2. Political and Economic Impacts of Cryptography

Governments regulate and control the use of cryptography in considerable part. The militarisation of cryptography and academic engagement in government projects highlight the political elements of cryptography practices. Moral dilemmas confront experts in the field, especially in the domains of national security and law enforcement, underline the need of nuanced regulatory frameworks controlling encryption technologies.

Significant economic consequences of cryptography are felt particularly in the software and banking industries. Using encryption technologies changes commercial procedures, legal requirements, and security protocols. The continuous talks about export laws, industry competitiveness, and developing safe transaction systems show the economic importance of encryption. As they advance, the financial effects of encryption technology on different industries emphasise the need for ethical considerations to direct their responsible use and regulation.

5. Case Studies

Case Study I : The Enigma Machine and its Impact on World War II

Introduction

The Enigma machine, which is a complex electromechanical cipher device, played an important and pivotal role in military personnels’s communication by encrypting the highly sensitive military messages, during World War II. Developed in the early 20th century, it was adopted by Nazi Germany during the War. Initially deemed unbreakable by the Germans, the Enigma's eventual cracking by Allied forces' codebreakers significantly impacted the war's course and the outcome.

Technology and Design

The Enigma machine utilized multiple rotors, each with internal wiring that scrambled letters differently with each keypress. This scrambling process, along with frequent changes in rotor settings and plugboard configurations, generated a billion possible code combinations, leading the Germans to believe it was unbreakable.

Key Features:

- **Rotors:** The core of the Enigma were its rotors, typically three or four in number, with internal wiring that substituted letters with each keypress.
- **Plugboard:** An additional layer of plugboard allowed users to manually swap specific pairs of letters before and after rotor encryption leading to much more complexity.
- **Reflector:** Reflector ,as the last stage, reversed the signal's path through the rotors, further obscuring the original message.

Cryptanalysis and Codebreaking

Despite all the complexity, the Enigma was not an unbreakable system. Several factors contributed to its eventual decryption:

- **Polish Intelligence:** Polish mathematicians Marian Rejewski, Jerzy Różycki, and Henryk Zygalski made initial breakthroughs in deciphering the Enigma's code during the early 1932 era itself.
- **British Codebreakers:** After invading Poland, the British at Bletchley Park received Polish intelligence on Enigma, which allowed them to build upon their work and develop more advanced cryptanalysis techniques for the same.
- **Human Error and Operational Flaws:** German reliance on the periodic key changes and operator errors provided critical clues to Allied codebreakers.

Historical and Strategic Impact

The decryption of Enigma messages codenamed as "Ultra",by the Allies, proved to be a major turning point in the war:

- **Strategic Intelligence:** Ultra provided crucial insights into German military plans, troop movements, and strategic intentions beforehand.
- **Battle Outcomes:** Deciphering Enigma messages played a decisive role in several key battles, including the Battle of the Atlantic , the D-Day landings etc.
- **Shortening the War:** Historians estimate that Ultra intelligence shortened the war by several years, saving at least millions of innocent lives.

Analysis using the STS Lens:

1. Social Construction of Technology (SCOT):

- The Enigma machine wasn't simply a technological marvel born out of nowhere; its development was shaped by the social context of pre-WWII Germany. The Nazi regime's emphasis on secrecy and control lead to the design and implementation of the Enigma, reflecting how the social forces can influences the course of the Technological Advancement

- The cracking of the Enigma code was again a product of the collaborative efforts of Polish and British codebreakers, highlighting how social networks and collaboration have always played a crucial role in technological breakthroughs.

2. Actor-Network Theory (ANT):

- The Enigma machine wasn't made in isolation. Rather, It existed due to the complex network of actors, including mathematicians, engineers, military personnel, and codebreakers. Each actor played their role in the development, use,

and eventual decryption of the Enigma, demonstrating the interconnectedness of various actors who shape the development around a technology.

- The network of actors involved in cracking the Enigma code, from initial Polish breakthroughs to the collaboration at Bletchley Park, exemplifies how technological advancements often emerge from the interactions and knowledge exchange between the different nodes in a diverse Network Society.

3. Feminist STS (Rosalind Williams View on the Technological Determination):

- The story of Enigma often focuses on male mathematicians and codebreakers, it's important to acknowledge the contributions of women like Mavis Lever who played significant roles in code breaking efforts at Bletchley Park.

- The Enigma case when viewed through a feminist lens encourages a more inclusive understanding of the human element within technological development and recognizes the diverse actors who contributed a lot to scientific and technological progress.

4. STS and Power:

- The Enigma machine developed as a tool of power for Nazi Germany, allowed them to encrypt sensitive military communications and maintain control over information. Highlights the inherent power dynamics associated with technological development and potential for its misuse.

- Successfully decrypting the Enigma code ultimately shifted the power balance in favor of the Allies, which demonstrated how technological advancements challenge and even disrupt existing power structures.

Case Study II : RSA and the Digital Revolution

The RSA algorithm was developed during the 1970s and marked a turning point in cryptography, paving the way for secure online communication and transactions in turn leading to the digital revolution.

RSA Algorithm:

- **Public-Key Cryptography:** In contrast to the traditionally used symmetric-key based cryptographic techniques which uses the same secret key for both encryption and decryption, RSA instead utilizes a separate public and private key pair.
- **Mathematical Foundation:** RSA relies on the NP-Hard complexity of factoring large prime numbers.
- **Key Generation:** A large public key and a corresponding private key are mathematically generated ,from two large prime numbers, which are further used for the encryption and the decryption of the same !
- **Encryption and Decryption:** Information encrypted with the public key can only be decrypted with the corresponding private key, ensuring secure communication.

Impact on the Digital Revolution:

- **Secure Communication:** RSA enabled secured online communication and also formed the foundation for protocols like HTTPS, which allows secure data transmission on websites.
- **Digital Signatures:** RSA allows for digital signatures which are today used for verifying the authenticity and integrity of digital documents and messages.
- **Key Infrastructure:** Public-key infrastructure (PKI) based on RSA facilitates secured communication and authentication across various online platforms in modern times.

- **E-commerce and Online Services:** The secure environment developed due to RSA fueled the growth of e-commerce, online banking, and other digital services.

Contribution:

- **Revolutionized Online Security:** Before the RSA was developed, secured online communication was largely unthinkable. RSA provided a robust and efficient solution, enabling the secure exchange of sensitive information over the internet.
- **Privacy and Trust:** Authenticity guaranteed by the RSA fostered the sphere of E-commerce and Online Transaction.
- **Foundation of Modern Cryptography:** RSA's principles became the underlying principle for various modern cryptographic algorithms and protocols, shaping the digital landscape we rely upon today.

Analysis:

1. Social Construction of Technology (SCOT):

- Similar to the Enigma Machines, RSA also emerged due to a specific social context, namely the growing need for secure online communication in the early stages of the internet.

- The widespread adoption of RSA and its integration into various online platforms like web browsers and email clients reflects the social construction aspect of this technology.

2. Actor-Network Theory (ANT):

- The RSA algorithm wasn't the sole invention of Researchers Rivest, Shamir, and Adleman. Its development and implementation involved a network of actors, includes other mathematicians, computer scientists, engineers, policymakers, and technology companies , as well . Each actor played a significant role in refining the algorithm.

- The widespread adoption of RSA across various sectors also demonstrates the interconnectedness of this technology within a vast network of actors and institutions.

3. Feminist STS:

- While the story of RSA is often focused on the male inventors, it's also very crucial to acknowledge the contributions of women like Whitfield Diffie and Hellman, whose work on public-key cryptography laid the groundwork for RSA which we today know as the Diffie-Hellman Algorithm.

4. STS and Power:

- The RSA algorithm empowered individuals and organizations to securely communicate and conduct transactions online, challenging the traditional control over information held by centralized entities leading to several changing Power dynamics.
- However, the widespread use of RSA also raises concerns regarding the major power imbalances. The control over private keys and access to decryption capabilities also grants significant power to individuals and organizations.

Case Study III : The Crypto Wars and the Clipper Chip

The Crypto Wars of the 1990s is a significant period in the debate between encryption and government control over digital communication. At the heart of this issue stood the Clipper Chip a controversial technology proposed by the US government.

The Clipper Chip:

- **Technology and Purpose:** Developed by the National Security Agency (NSA), the Clipper Chip is a microchip designed for mobile phones implementing strong encryption but with a crucial caveat: a "key escrow" system , which will allow the govt to access the encrypted information as well for investigative purposes.

- **Key Escrow:** Each Clipper Chip contains a copy of its decryption key which is also stored within a government central repository. This backdoor aims to grant law enforcement access to encrypted communications for investigative purposes.

Opposition and Public Outcry:

- **Privacy Concerns:** The Clipper Chip faced fierce opposition from civil liberties groups, technologists, and the public themselves. As the system raised significant concerns about government surveillance, potential abuse of power, and the erosion of individual privacy in the digital age.
- **"Code is Speech" Argument:** Cryptography experts like Phil Zimmermann of the Electronic Frontier Foundation (EFF) argued that strong encryption was essential for a free and open internet. They championed the idea that "code is speech," protected by the First Amendment, and that government control over encryption undermined the notion of the free expression.

The Outcome:

- **Market Failure:** Despite all the government pressure, Clipper Chip failed to gain any widespread adoption as such. Since , most Phone manufacturers and consumers were hesitant to embrace technology with a built-in backdoor, leaving the initiative commercially unviable.
- **Export Controls:** The Crypto Wars also made the US government put restrictions on the export of strong encryption technologies. This policy was aimed at limiting the spread of encryption tools deemed beneficial to criminals and terrorists.

Legacy of the Crypto Wars:

- **Victory for Strong Encryption:** So-called “Crypto Wars” ultimately resulted in a significant victory for strong encryption and the protection of individual privacy in the digital realm. The Clipper Chip project was finally abandoned.
- **Ongoing Debate:** While the Crypto Wars established strong encryption as a cornerstone of digital security, the tension between privacy and national security still persists till today as the Governments continue to seek ways to balance the need for law enforcement access with the protection of individual privacy.

Analyzing the Crypto Wars of the 1990s through STS Frameworks:

1. Social Construction of Technology (SCOT):

- The Clipper Chip isn’t simply a technological innovation formed out in isolation; rather, it is a product of the social and political context of the 1990s which is centered around the growing concerns about national security in the wake of terrorist attacks and the rise of digital communication.
- The public outcry/protests leading to the eventual failure of the Clipper Chip astoundingly demonstrates how social forces (including the mass public opinion, civil liberties movements, and technological expertise) can shape and ultimately reject technologies perceived as a threat to individual privacy and freedom.

2. Actor-Network Theory (ANT):

- The Clipper Chip isn't an invention in isolation. Rather a product formed by a network of actors, including government agencies like the NSA, technology developers, phone manufacturers, civil liberties groups, and the general public.
- Crypto Wars through ANT perfectly highlights the interconnectedness of actors with their diverse interests and displays the power dynamics at play. When the government sought control through the Clipper Chip, civil liberties groups and technologists formed their own counter-network advocating for a strong encryption and individual privacy.

3. STS and Power:

- Similar to the previous case studies example , the Clipper Chip shows the government's idea to maintain control over encrypted communication for national security purposes, potentially also infringing upon individual privacy and freedom of expression.
- On the other hand, public opposition and eventual failure of the Clipper Chip demonstrates the power of collective action in challenging the government’s overreach.

Case Study IV : Cryptographic Techniques in the field of Bitcoin and Blockchain

1. **Digital Signatures:**
    - As cited in the previous Case Studies ,Public-key cryptography most based on AES , influenced by RSA, forms the backbone of Bitcoin and blockchain security. Wherein each user possesses a public and private key pair.
    - When a user initiates a Bitcoin transaction, they sign it with their private key, in turn creating a unique digital signature for themselves.

    - This signature later on helps to verify the authenticity and the origin of the transaction, ensuring it hasn't been tampered.
2. **Hashing:**
    - Cryptographic hashing function plays a very crucial role in creating a tamper-proof record of the transactions as a ledger on the Blockchain (registry).
    - Each block on the blockchain contains the hash of the previous block, forming a chain with a unique fingerprint, which is generated through Mining and acts as Proof-Of-Work.
    - Any attempt to alter a transaction within a block would change its hash, making it instantly detectable by the network, which makes it difficult to start a cyber attack on the network.
3. **Elliptic Curve Cryptography (ECC):**
    - Bitcoin along with many other similar blockchain networks utilize the ECC technique for public-key cryptography due to its efficiency and smaller key sizes..
    - This in turn allows for faster and more lightweight cryptographic operations on the network.

Impact of Encryption Techniques:

- **Security and Immutability:** These cryptographic techniques ensure the security and immutability of the blockchain. Transactions are verifiable and tamper-proof, fostering trust and transparency within the Bitcoin network and it’s users.
- **Decentralization:** By eliminating the need for a central authority for verification and other management , cryptography empowers a distributed network to validate and secure transactions. This also influences the power dynamics of the centralised authorities.

- **Pseudonymity:** Although Bitcoin transactions are publicly viewable, user identities still remain pseudonymous through their public key addresses, offering a degree of privacy.

Case Study V : WhatsApp Encryption

Signal and WhatsApp, are the two popular real time-messaging platforms today , which prioritize the user's privacy by utilizing end-to-end encryption (E2EE) for communication.

Specific Cryptographic Algorithms:

Both Signal and WhatsApp majorly rely on the **Open Whisper Systems (OWS) library** for their E2EE implementation. This library utilizes a combination of algorithms for secure communication:

- **Symmetric Encryption:**
    - Advanced Encryption Standard (AES) with 256-bit keys is used to encrypt the message content itself.
    - This ensures that only the sender and intended recipient can decrypt and read the message.
- **Asymmetric Encryption:**
    - A combination of Curve25519 for key exchange and XEdDSA for digital signatures is employed in this layer.Due to this the secure key exchange and message authentication, ensuring messages haven't been tampered with during transmission becomes a possibility.

Challenges to User Privacy:

Despite robust encryption, maintaining complete user privacy faces several challenges:

- **Metadata Collection:** While message content is encrypted, metadata like sender/receiver information, timestamps, and message size remain unencrypted. This metadata can potentially reveal communication patterns and user behavior.
- **Government Backdoors:** Governments often pressure messaging platforms to implement backdoors or weaken encryption protocols for easier access to encrypted messages for law enforcement purposes. This raises significant privacy concerns and undermines the core principle of E2EE.
- **Vulnerability to Hacking:** While the encryption itself is robust, platforms are still susceptible to hacking attempts that could compromise user data and encryption keys.

Balancing Security and Legal Requirements:

The ongoing debate revolves around finding a balance between user privacy and national security:

- **Privacy Advocates:**
    - They argue that strong encryption is essential for protecting individual privacy and freedom of expression in the digital age.
    - Backdoors and weakened encryption protocols create vulnerabilities and set a dangerous precedent for government surveillance.
- **Law Enforcement Agencies:**
    - They emphasize the need for access to encrypted communication in the fight against terrorism and criminal activity.
    - They argue that some form of legal framework is necessary to enable investigations and prevent the spread of illegal content.

Analyzing Signal and WhatsApp's E2EE through an STS Lens:

1. Social Construction of Technology (SCOT):

- The development and widespread adoption of E2EE messaging platforms like Signal and WhatsApp weren't solely driven by technological advancements. They emerged from a growing social demand for secure communication in the digital age, fueled by concerns about government surveillance and data breaches.
- The success of these platforms relies on the social construction of trust in their encryption protocols. Users trust that their messages remain private and unreadable by anyone except the intended recipient, including the platforms themselves.

2. Actor-Network Theory (ANT):

- E2EE messaging platforms like Signal and WhatsApp are not solely the product of their developers. They exist within a complex network of actors, including users, governments, law enforcement agencies, technology companies, and civil liberties groups. Each actor has a stake in the functionality and privacy guarantees offered by these platforms.
- Analyzing E2EE through ANT highlights the ongoing tension between these actors. Users and privacy advocates prioritize strong encryption and user privacy, while governments and law enforcement agencies seek ways to balance security needs with access to encrypted communication for investigative purposes.

3. Feminist STS:

- While the development of E2EE protocols often focuses on male technologists, it's crucial to acknowledge the contributions of women like Moxie Marlinspike, co-founder of Open Whisper Systems, whose work has been instrumental in advancing secure communication technologies.

4. STS and Power:

- By encrypting communication and limiting access to message content, these platforms empower individuals to control their privacy and engage in communication free from government surveillance.
- Governments and law enforcement agencies hold significant power in pressuring platforms to weaken encryption or implement backdoors, potentially infringing upon individual privacy rights.

Case Study VI : Cryptography for the Cloud Data Storage

Cloud storage services like Google Drive and Dropbox offer convenient and scalable storage solutions for individuals and organizations. However, entrusting sensitive data to a third-party provider often necessitates robust security measures to ensure data confidentiality and integrity.

Leveraging Cryptography for Data Security:

Cloud storage providers employ various cryptographic techniques to safeguard user data:

- **Encryption Standards:**
    - Data at rest is typically encrypted using industry-standard algorithms like AES-256, ensuring only authorized users can access it.
    - Data in transit is often protected by TLS/SSL protocols, encrypting communication between user devices and the cloud storage infrastructure.
- **Key Management:**
    - Cloud providers offer different key management options:

    - **Server-Side Encryption (SSE):** The provider manages encryption keys, offering convenience but raising concerns about potential access by the provider itself.
    - **Client-Side Encryption (CSE):** Users manage their own encryption keys, providing greater control but requiring additional user responsibility.

Potential Vulnerabilities and Security Breaches:

Despite robust encryption, cloud storage systems are not immune to security threats:

- **Misconfigurations:** Improper configuration of encryption settings or access controls can create vulnerabilities exploitable by attackers.
- **Insider Threats:** Malicious actors within the cloud provider or authorized users with elevated access privileges can potentially compromise data security.
- **Data Breaches:** External attacks targeting cloud storage infrastructure or user accounts can lead to data breaches and unauthorized access.

Importance of User Awareness:

While cloud providers implement strong security measures, user awareness plays a crucial role in data protection:

- **Strong Passwords:** Using strong and unique passwords for cloud storage accounts is essential to prevent unauthorized access.
- **Two-Factor Authentication (2FA):** Enabling 2FA adds an extra layer of security, requiring additional verification beyond just a password.
- **Selective Sharing:** Users should carefully consider who they share their data with and avoid oversharing sensitive information.

- **Regular Backups:** Maintaining backups of critical data outside the cloud storage platform provides an additional layer of protection in case of data loss.

Analysis using the STS Lens:

1. Actor-Network Theory (ANT):

- Cloud storage security involves a complex network of actors, including cloud providers, users, governments, and regulatory bodies. Each actor plays a role in shaping the security landscape:
    - Cloud providers implement various cryptographic techniques and security protocols to safeguard data.
    - Users share their data with these platforms, relying on their security measures.
    - Governments and regulatory bodies establish legal frameworks and standards for data protection, influencing the security practices of cloud providers.
- Analyzing cloud storage through ANT highlights the shared responsibility for data security. While providers implement robust encryption, user awareness and responsible data management practices are crucial, and governments play a vital role in establishing legal frameworks that hold providers accountable for data security.

2. STS and Power:

- Cloud storage platforms hold significant power over user data. Encryption and access controls determine who can access and utilize the stored information. This raises concerns about potential power imbalances and the need for transparency and accountability in data handling practices.
- The debate surrounding key management options (SSE vs. CSE) highlights the power dynamics between cloud providers and users. While SSE offers

convenience, it grants providers control over encryption keys, raising concerns about potential access and potential conflicts with user privacy rights.

Case Study VII: Apple vs. FBI: A Clash over Terrorism and Data Privacy in 2016

The Apple vs. FBI case of 2016 marked a pivotal moment in the ongoing debate between encryption, data privacy, and national security.

Background:

Following the San Bernardino terrorist attack in December 2015, the FBI sought access to data on the iPhone belonging to one of the perpetrators. However, the phone's strong encryption rendered it inaccessible without the passcode. The FBI requested Apple's assistance in creating a custom iOS version that would bypass the security features, allowing them to brute-force the passcode.

Apple's Refusal and Arguments:

Apple vehemently opposed the FBI's request, citing the following arguments:

- **Security Risks:** Creating a backdoor for this specific case would set a dangerous precedent, making all iPhones vulnerable to future government intrusion and potentially jeopardizing user data security.
- **Unconstitutional Order:** Apple argued that the court order compelling them to create the hacking tool violated the First Amendment (protecting freedom of speech) and the Fifth Amendment (protection against self-incrimination).

- **No Legal Basis:** The All Writs Act, cited by the FBI, was not intended to force companies to create new software for law enforcement purposes.

Public Debate and Outcome:

The case ignited a heated public debate between:

- **National Security Advocates:** They argued that law enforcement agencies require access to encrypted data to investigate serious crimes and prevent future attacks.
- **Privacy Advocates:** They emphasized the importance of strong encryption for protecting individual privacy and freedom from government overreach.

Ultimately, the case took an unexpected turn. The FBI announced they had successfully unlocked the phone with the help of a third-party vendor, prompting them to withdraw their request from Apple. The details of the method used remain classified.

Implications and Lasting Impact:

While the immediate legal battle ended, the Apple vs. FBI case left a lasting impact:

- **Heightened Awareness of Encryption Debate:** The case brought the issue of encryption and its implications for both security and privacy to the forefront of public discourse.
- **Ongoing Tension:** The tension between national security needs and individual privacy rights continues to be a point of contention, with governments seeking ways to balance both.
- **Importance of Strong Encryption:** The case reaffirmed the importance of strong encryption for protecting user data and fostering trust in the digital world.

Analyzing the Apple vs. FBI Case through an STS Lens:

1. Social Construction of Technology (SCOT):

- The case wasn't solely about the technical feasibility of unlocking the iPhone. It highlighted the social context of the post-9/11 era, where national security concerns heightened the demand for law enforcement access to encrypted data. However, this demand clashed with the growing societal value of individual privacy and the need for secure communication in the digital age.

2. Actor-Network Theory (ANT):

- The case involved a complex network of actors:
    - Apple represented the technology company and its responsibility to protect user data and security.
    - The FBI represented the law enforcement agency seeking access to information for investigative purposes.
    - The public played a crucial role in voicing their opinions and shaping the public discourse around the case.
    - The legal system, through the court order, attempted to mediate the clash between these actors.
- Analyzing the case through ANT reveals the power dynamics at play. Apple resisted the government's pressure to create a backdoor, highlighting the potential for technology companies to act as gatekeepers of user data and security.

6. References

1) Slides given by our Professor - Dr. Radhika Krishnan for the course - Science , Technology and Society
2) Abbasi, G., Tiew, L., Tang, J., Goh, Y., & Thurasamy, R. (2021). The adoption of cryptocurrency as a disruptive force: Deep learning-based dual stage structural equation modelling and artificial neural network analysis. *PLoS ONE*, 16. https://doi.org/10.1371/journal.pone.0247582.
3) Fulk, J., Schmitz, J., & Ryu, D. (1995). Cognitive Elements in the Social Construction of Communication Technology. *Management Communication Quarterly*, 8, 259 - 288. https://doi.org/10.1177/0893318995008003001.
4) *Cryptology | Definition, Examples, History, & Facts*. (1999, July 26). Encyclopedia Britannica. https://www.britannica.com/topic/cryptology/History-of-cryptology
5) Wikipedia contributors. (2024, March 20). *History of cryptography*. Wikipedia. https://en.wikipedia.org/wiki/History_of_cryptography
6) Sidhpurwala, H. (2024, April 30). A Brief History of Cryptography. *RedHat*. https://www.redhat.com/en/blog/brief-history-cryptography
7) Doumenjou, J. (2022, November 16). *The evolution of cryptography in modern History*. Traefik Labs: Say Goodbye to Connectivity Chaos. https://traefik.io/blog/the-evolution-of-cryptography-in-modern-history/
8) *A brief history of encryption (and cryptography)*. (2023, February 1). Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption
9) Decentriq. (2018, December 3). *The evolution of cryptography (deciphered)*. https://www.decentriq.com/article/evolution-of-cryptography
10) Wikipedia contributors. (2024b, April 27). *Cryptanalysis*. Wikipedia. https://en.wikipedia.org/wiki/Cryptanalysis
11) Dahan, M., & Dahan, M. (2023, November 17). *Cryptanalysis explained*. Comparitech. https://www.comparitech.com/blog/information-security/cryptanalysis/
12) Regalado, A. (2020, April 2). Cryptographers have an ethics problem. *MIT Technology Review*. https://www.technologyreview.com/2013/09/13/15059/cryptographers-have-an-ethics-problem/
13) Santa Clara University. (n.d.). *Ethical questions about encryption*. Markkula Center for Applied Ethics. https://www.scu.edu/ethics/focus-areas/technology-ethics/resources/ethical-questions-about-encryption/
14) Wikipedia contributors. (2024c, May 5). *Enigma machine*. Wikipedia. https://en.wikipedia.org/wiki/Enigma_machine

15) Wikipedia contributors. (2023, July 28). *Clipper chip*. Wikipedia. https://en.wikipedia.org/wiki/Clipper_chip
16) GeeksforGeeks. (2022, September 20). *Cryptography in Blockchain*. GeeksforGeeks. https://www.geeksforgeeks.org/cryptography-in-blockchain/
17) Upadhyay, S., & Gupta, V. K. (2022). A LITERATURE REVIEW ON THE CONCEPT OF CRYPTOGRAPHY AND RSA ALGORITHM. *ResearchGate*. https://www.researchgate.net/publication/360175324_A_LITERATURE_REVIEW_ON_THE_CONCEPT_OF_CRYPTOGRAPHY_AND_RSA_ALGORITHM
18) Bhargav, A., & Manhar, A. (2020). A review on cryptography in cloud Computing. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 225–230. https://doi.org/10.32628/cseit206639

7. Contributions

- **Aishani Pandey (2022121009)** - Did Introduction(Heading 1) and Theoretical Frameworks (Heading 3)
- **Ayush Maurya (2021115004)** - Did Historical Context and Development(Heading 2) and Critical Analysis(Heading 4)
- **Harshvardhan (2021111017) -** Report analysis for writing the relevant Case Studies