PROJECT - Science, Technology and Society

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

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

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. Theoretical Frameworks

2.1. 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.

2.1.1. Interpretative Flexibility

Interpretative flexibility refers to the notion that different social groups can have divergent 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 personal data, privacy, and 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.

2.1.2. 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.

2.1.3. 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.

2.1.4. 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.

2.1.5. 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.

2.2. 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.

2.2.1. 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.

2.2.2. 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.

2.2.3. 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.

2.2.4. 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

2.2.5. 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

2.2.6. 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.

2.3. 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.

2.3.1. 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.

2.3.2. 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.

2.3.3. 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 .

2.3.4. 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.

2.3.5. 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.

3. 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)

4. Contributions

- **Aishani Pandey (2022121009)** - Did Introduction(Heading 1) and Theoretical Frameworks (Heading 3)