Global Encryption Coalition

Internet Society Foundation

Internet Society Armenia Chapter

# YEREVAN, ARMENIA
# OCTOBER 4, 2024
# ENCRYPTION: A DIGITAL SECURITY FACTOR

REPORT

# *OBJECTIVES*

- **Raise Awareness**. Educate participants on the importance of encryption for securing personal data and online communications.
- **Discuss Challenges and Opportunities.** Explore the current state of encryption technologies and their potential for improving cybersecurity in Armenia.
- **Policy and Legislation.** Engage stakeholders in discussions on aligning Armenia's encryption policies with global standards.

- **Promote Encryption.** Encourage individuals, businesses, and institutions to adopt encryption tools for secure communication.
- **Foster Collaboration.** Build networks between tech, government, and civil society to advocate for strong encryption policies.

Internet Society
Armenia Chapter

# *DESCRIPTION*

On the occasion of Global Encryption Day on October 4, a workshop titled **“Encryption: A Digital Security Factor”** was organized by the Internet Society Armenia Chapter PO. The event was attended by representatives of the technical community.

Leading experts in the field discussed the security of personal, commercial, and other types of data, as well as the various factors that threaten them. Encryption Day in Armenia within the framework of Global Encryption Day took place with the agenda:

- **What is ransomware and how can you protect yourself**
- **Post-Quantum Encryption (PQC)**
- **Coding in e-government and digital governance**
- **Coding in the financial sector**
- **Encryption and cybersecurity challenges**

Internet Society
Armenia Chapter

# *OPENING REMARKS*

Igor Mkrtumyan, the President of the Internet Society Armenia Chapter PO, provided an in-depth discussion on current global trends in data protection and encryption, emphasizing the critical role of encryption in safeguarding personal data and securing digital communications in today's interconnected world. He highlighted the importance of addressing encryption challenges collaboratively, as these issues often require the combined expertise and coordinated actions of the professional community across disciplines and sectors. secure digital environment.

Mr. Mkrtumyan underscored that the workshop's goal extends beyond merely sharing information; it aims to foster a stronger, more resilient technical community that can respond to evolving threats in data security. Additionally, he pointed out the importance of raising public awareness around encryption, helping the general population understand how encryption protects their privacy and the overall digital ecosystem. By bridging the knowledge gap and promoting open dialogue, the workshop seeks to encourage greater adoption of secure practices among individuals and organizations alike, paving the way for a more secure digital environment.

***Igor Mkrtumyan, President of the Internet Society Armenia Chapter***

Internet Society
Armenia Chapter

# *TOPICS AND SPEAKERS*


***Areg Shmavonyan, InfoTec Cybersecurity LLC***

## Encryption and measures to prevent the spread of Ransomware crypto viruses

The Ransomware crypto virus spread to 150 countries within a few days, infecting 200,000 computers. The direct damage amounted to $4 billion, while the consequential damage reached $7 trillion.
This crypto virus encrypts all types of files and restricts access to the computer, demanding a "ransom" in cryptocurrency to restore data and access. It spreads rapidly and automatically, targeting all types of devices. Networks are primarily accessed through phishing emails, infected USB flash drives, and other similar methods.
Cybersecurity Engineer **Areg Shmavonyan** discussed preventive measures to avoid ransomware during the workshop.

Mr. Shmavonyan addressed the common methods through which ransomware infiltrates systems, underscoring key attack vectors such as:

**Phishing Emails:** These are deceptive emails designed to trick recipients into clicking malicious links or downloading infected attachments, thereby compromising their systems.
**Malicious Websites:** Unsecured or fraudulent websites can contain harmful code that automatically installs ransomware when users visit them.
**Infected Software:** Downloading software from unverified sources can result in hidden malware being installed alongside the intended application, enabling ransomware to spread.
**USB Drives:** Physical media like USB drives, especially those of unknown origin, can carry malware that installs ransomware when plugged into a computer.

He emphasized that the best defense against ransomware is vigilance. Avoiding suspicious emails, unknown links, and unverified software sources can significantly reduce the risk of infection. Staying aware and cautious is essential for protecting personal and organizational data against ransomware threats.

Internet Society
Armenia Chapter

# *THE REAL COSTS OF RANSOMWARE ATTACK*

Financial Loss Ransom payments Downtime and lost productivity Recovery costs

Data Loss Permanent loss of critical files Risk of data corruption or destruction

Reputation Damage Legal consequences due to data breaches

Regulatory Fines Violations of data protection laws (GDPR, HIPAA, etc.) Failure to meet compliance standards

Business Disruption Delayed operations Potential bankruptcy for small businesses

Internet Society
Armenia Chapter

# *HOW TO SECURE YOUR DATA*

**Regular Backups**
Keep frequent backups of your files in offline or cloud storage

**Email Awareness**
**Be cautious of phishing emails.**

**Update Software**
**Ensure all software, including operating systems and antivirus, are updated regularly.**

**Network Segmentation**
Isolate critical systems and data from other parts of the network.

Internet Society
Armenia Chapter

# *POST-QUANTUM CRYPTOGRAPHY*

Sergey Abrahamyan, professor of the Institute for Informatics and Automation Problems, talked about types of cryptography.

***Symmetric***

- Allows two parties to communicate secretly on a public channel, only if they exchanged a secret key on a private channel before
- Efficient both in hardware and software
- Usually more trusted

***Asymmetric***

- Allows two parties to communicate secretly on a public channel, even if they never communicated before
- Significantly less efficient than symmetric crypto
- Based on mathematical problems that are hard to solve

Internet Society
Armenia Chapter

# *POST-QUANTUM CRYPTOGRAPHY*

**Mr. Abrahamyan** also highlighted that quantum cryptography, in its practical applications today, is mostly limited to quantum key distribution (QKD), a method that enables secure key exchange between parties. However, it faces several notable limitations.

One primary issue is the lack of built-in authentication mechanisms, which means there's no inherent way to verify the identities of the parties involved in communication. While certain technologies, like physical unclonable functions (PUFs), can offer authentication, these are not standard in all implementations of quantum cryptography.

Another significant challenge is the requirement for a direct, fiber-optic connection or an unobstructed line of sight between the communicating parties, which restricts its use to specific environments. Quantum cryptography also has difficulty maintaining signal integrity over long distances, resulting in limited range without substantial data loss. Additionally, deploying quantum cryptography requires entirely new infrastructure and technology, as it cannot operate over existing digital networks.

# *POST-QUANTUM CRYPTOGRAPHY*

Its practical application is further limited by its incompatibility with mobile devices, sensor networks, and other systems that rely on wireless communication or portability, such as connected cars. Finally, scaling quantum cryptography to large networks or multi-user environments remains a major challenge, making it less feasible for widespread, flexible use.

**Post-Quantum Cryptography (PQC)** is based on classical algorithms specifically designed to withstand the potential threats posed by quantum computers. These algorithms are efficient on conventional computers, meaning they can run effectively without requiring excessive time, memory, or communication resources. Importantly, they are also designed to be resilient against attacks from both classical and quantum algorithms, making them robust in the face of future technological advances.

Unlike traditional cryptographic systems, PQC relies on mathematical problems that differ fundamentally from integer factorization or discrete logarithms—the basis for many current encryption methods. By leveraging alternative mathematical structures, PQC aims to provide security that remains reliable even as quantum computing technology evolves.

# *ENCRYPTION IN E-GOVERNMENT AND DIGITAL GOVERNANCE*

Information about encryption in E-Government and Digital Governance was provided by **Yeghisabet Alaverdyan Head of Systems Integration Department EKENG CJSC.**

E-Government refers to the use of digital technologies to provide government services and facilitate interaction with citizens, businesses, and other government agencies.
The main goal is to enhance transparency in governance.

**Core Concepts:**

- Digital Services: Offering public services online, like filing taxes, applying for permits, or voting.
- Citizen Engagement: Using digital platforms to involve citizens in decision-making processes & improve communication.
- Data Transparency: Individuals and businesses know what data is being collected, who can access it, how it's being used and how they can interact with it.
- Interoperability: Seamless sharing of information between different government systems and agencies.
- Security and Privacy: Protecting citizens' data and ensuring secure digital transactions.

# *ENCRYPTION IN E-GOVERNMENT AND DIGITAL GOVERNANCE*

## Key Components of Digital governance

**Digital Infrastructure:** Ensuring widespread access to the internet and digital devices so that citizens can participate in E-Government services.

**E-Services:** The various online services provided to citizens, businesses, and government employees.

**Digital Identity:** Secure and verifiable identities (e.g., electronic ID cards) enable users to authenticate themselves for various government services.

**Regulatory Frameworks:** Policies and regulations that ensure the ethical use of digital tools, protect user privacy and secure government information.

Internet Society
Armenia Chapter

# *ENCRYPTION IN E-GOVERNMENT AND DIGITAL GOVERNANCE*

Digital Governance **(DG)** seeks to ensure that all individuals have access to digital services and that their rights are protected in the digital space. This includes:

- promoting internet access,
- ensuring freedom of expression online,
- protecting digital identities,
- safeguarding users from online harassment or surveillance.

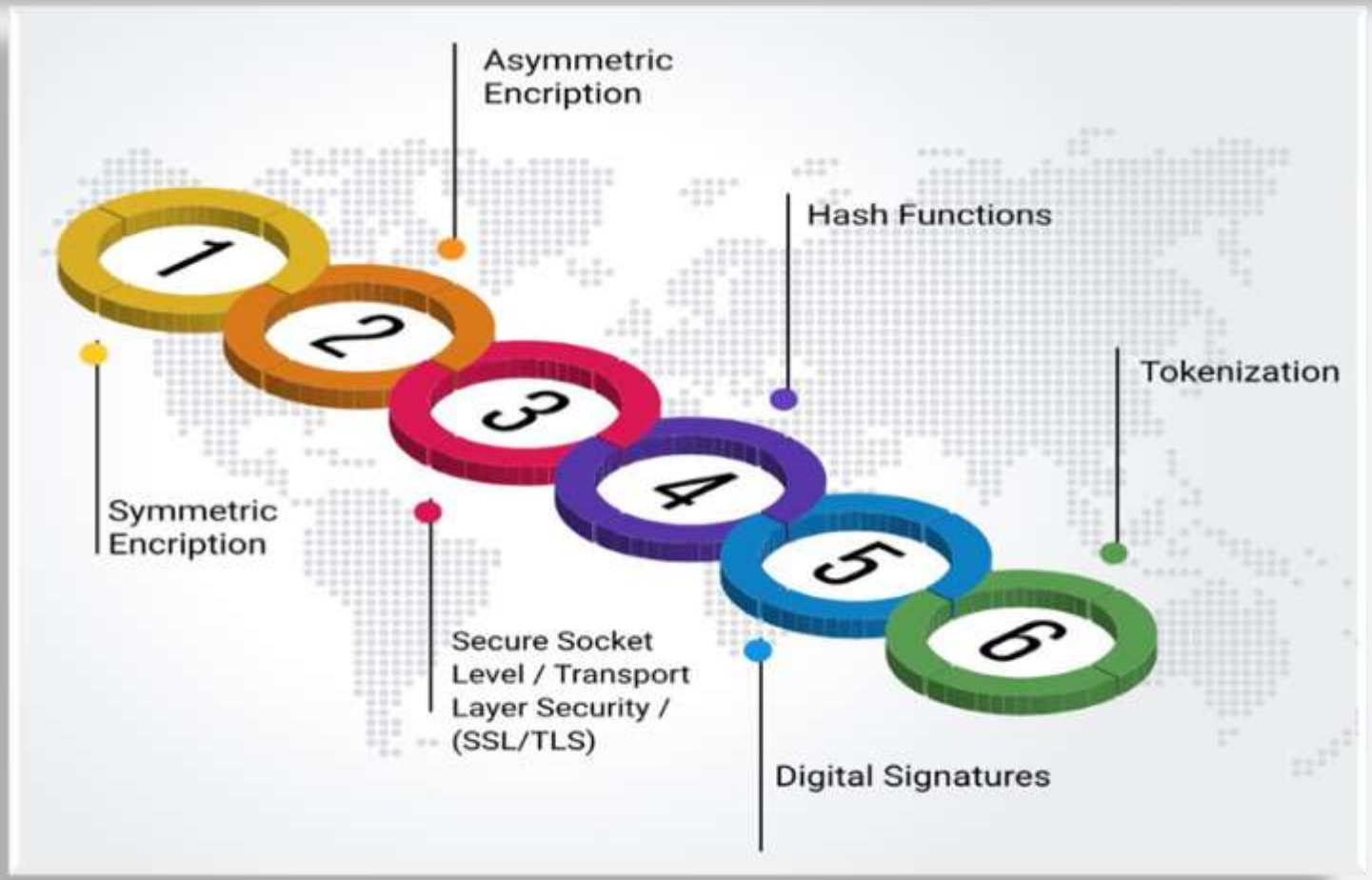
So, **E-Gov** is about implementing technology in government services, while concerns the managing digital transformation across all sectors.

***As governments become more reliant on digital infrastructures, ensuring the security and privacy of sensitive data has never been more critical.***
***This is where ENCRYPTION plays a pivotal role!***

***The three states of data***

- *Data at rest: encryption helps*
- *Data in transit: encryption helps*
- *Data in use: encryption does not help*

# *ENCRYPTION IN THE FINANCIAL SECTOR*




**Karen Yerznkanyan**, Central Depositary of Armenia, Information Security Officer talked about the encryption techniques for financial transactions.

# *BEST PRACTICES FOR ENSURING FINANCIAL INFORMATION PROTECTION*

- Enable Two Factor Authentication
- Encrypt Data in Transit and Rest
- Regularly Security Audit
- Implement Strong Password Policy
- Regularly Update and Patch Software
- Educate Users on Phishing and Social Engineering
- Monitor and Detect Anomalies

# *BEST PRACTICES FOR ENSURING FINANCIAL INFORMATION PROTECTION*

Strengthening fraud detection, improving privacy, and getting ready for potential threats are the main focuses of new trends in financial security. While blockchain and distributed ledger technologies offer safe, transparent records, artificial intelligence and machine learning are now being employed to identify fraud in real time.

Additional security layers are added via biometric authentication and Zero Trust architectures, which shield networks and accounts from unwanted access. To protect data from potential risks from quantum computing, post-quantum cryptography is being used, and privacy-enhancing technologies like homomorphic encryption guarantee compliance without risking sensitive data. In the digital age, these developments are crucial for creating safe and robust financial systems.


Internet Society
Armenia Chapter

# *THANK YOU*

Global Encryption Coalition

Internet Society
Armenia Chapter