NC Department of Health and Human Services

Information Technology Division
Privacy and Security Office

July 10, 2025

The DHHS Privacy and Security Office

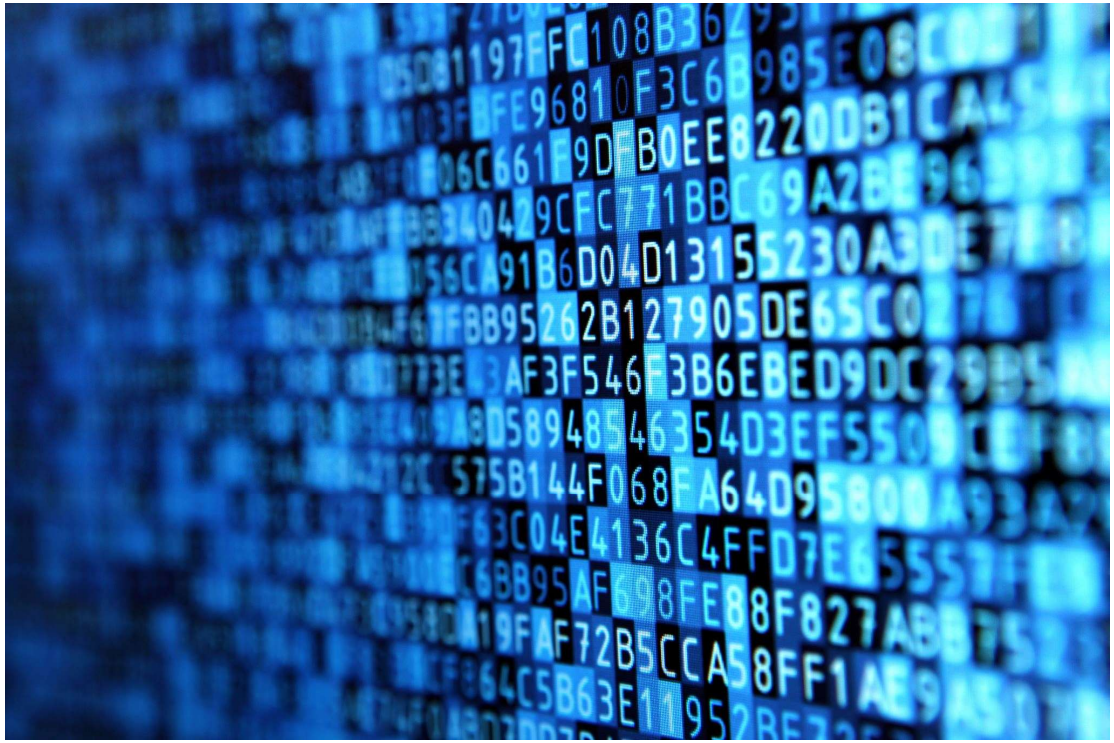
- The Privacy and Security Office (PSO) provides privacy and security information for the Department of Health and Human Services (DHHS). The PSO safeguards information from unauthorized use, disclosure, modification, damage or loss.
- The PSO provides consulting services around Privacy and Security, Business Continuity Planning (BCP), Continuity of Operations (COO), Disaster Recovery (DR), Forensic Investigations, Privacy and Security Policies, Incident Management, Risk and Threat Management.
- The PSO serves as the liaison between various Federal and State Agencies.
- The PSO is responsible for conducting annual reviews based on Federal and State requirements.

What is cryptography?

- According to the Oxford Dictionary it is the art of writing or solving codes.
- It is the practice of securing communication and data by transforming information into an unreadable format, known as ciphertext, using algorithms and keys.
- The cryptographic process is called encryption, which ensures only authorized parties with the correct decryption key can access the original, readable information, called plaintext.

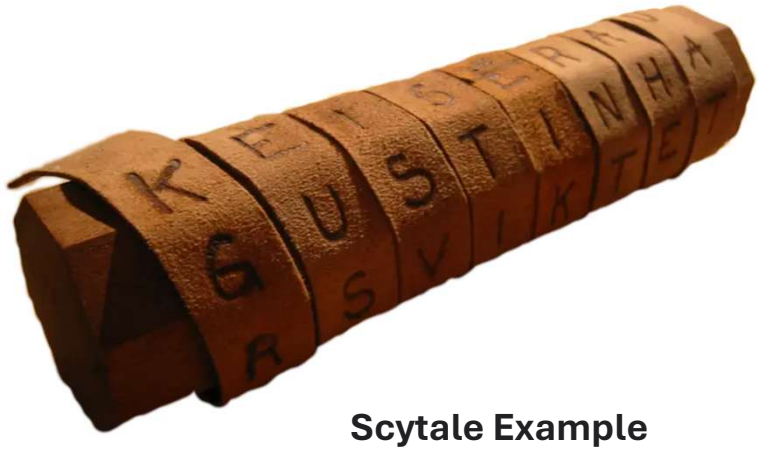
What is cryptography?

- The encrypted text is called ciphertext.
- Modern digital encryption is designed to prevent both humans and machines from the reading of data or information.



Cryptography 101

- Where did it originate?
- The first forms of encryption were simple substitution ciphers and transposition ciphers.



Scytale Example

- Scytale was a tool used to perform a transposition cipher, consisting of a rod, staff or other cylindrical object where a strip of material (e.g., leather or parchment) wound around.
- The message to be encrypted was written while the object was wrapped then removed and sent to the intended recipient.

Cryptography 101

- The Culper Ring and Code Book
  - Facilitated by two (2) individuals neither of which did any spying, but rather organized information and made sure it got to Washington.
  - The Ring operated for five (5) years until the end of the Revolutionary War and was considered far more successful than any other intelligence network during that time.
  - The book was a collection of 763 numbers.
    - 710 represented specific words.
    - The other 53 numbers were for names and places.
    - The book served as the encryptions key

Cryptography 101

- It is considered a key component in the CIA information security triad.

- **Confidentiality:**
  Cryptography ensures that only authorized individuals can access and understand the information, preventing eavesdropping and unauthorized access.

- **Integrity:**
  Cryptography can also help verify that data hasn't been tampered with during transmission or storage. With proper and working cryptography if data is altered, the cryptographic process can reveal the changes.

Cryptography 101

- Cryptography is not just encryption and includes Hashing.

- **Hashing:**
  The process of converting any piece of data, using an algorithm, into a typically much smaller “unique” identifier (i.e., Hash)

- They require the use of the same algorithm for validation.

- Hashes can be compared and will result in a match if the data is the same or mismatch if it’s changed.

Symmetric and Asymmetric

- **Symmetric:**
  A single secret key is shared between the sender and the receiver. The sender encrypts the data (plaintext) using this key, and the receiver then uses the same key to decrypt the ciphertext (encrypted data) back into the plaintext.

- **Asymmetric:**
  A pair of mathematically related keys one (1) private and one (1) public. The public key for encryption and a private key for decryption.

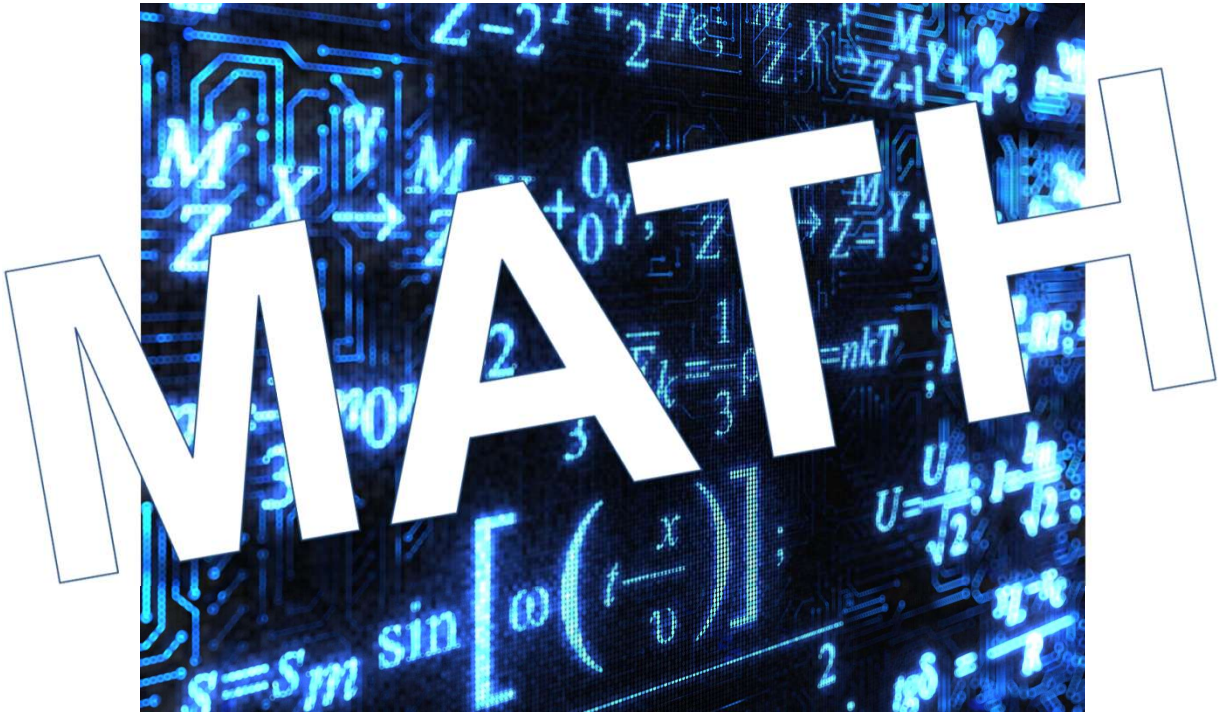
TLS and HTTPS

- **Transport Layer Security (TLS):**
  A security protocol designed to facilitate privacy and data security for communications over the Internet.

- **HTTPS:**
  Is an implementation of TLS encryption on top of the HTTP protocol, which is used by all websites as well as some other web services.

Cryptography 101

In depth analysis of cryptographic algorithms and how they work



Cryptography and North Carolina

- SCIO-SEC-316: System and Communications Protection Policy (SC)
  - SC-12 – Cryptographic Key Establishment and Management
  - SC-13 – Cryptographic Protection

FIPS Levels

- **Level 1:** The lowest level, requiring production-grade equipment and externally tested algorithms.
- **Level 2:** Adds requirements for physical tamper-evidence and role-based authentication.
- **Level 3:** Adds requirements for physical tamper-resistance and identity-based authentication.
- **Level 4:** The highest level, offering the most stringent physical security and robustness against environmental attacks.

FIPS 140-2

- U.S. government standard that specifies security requirements for cryptographic modules used to protect information.
- Issued and owned by the National Institute of Standards and Technology (NIST).
- It's a benchmark for validating the effectiveness of cryptographic hardware and software.
- FIPS 140-2 is being phased out, with all validations being retired (placed on the historical list) by September 21, 2026

FIPS 140-3

- Extends the cryptography standard beyond hardware to include both firmware, software, and hybrid modules

- Security requirements are now defined starting with the initial design all the way through operational deployment.

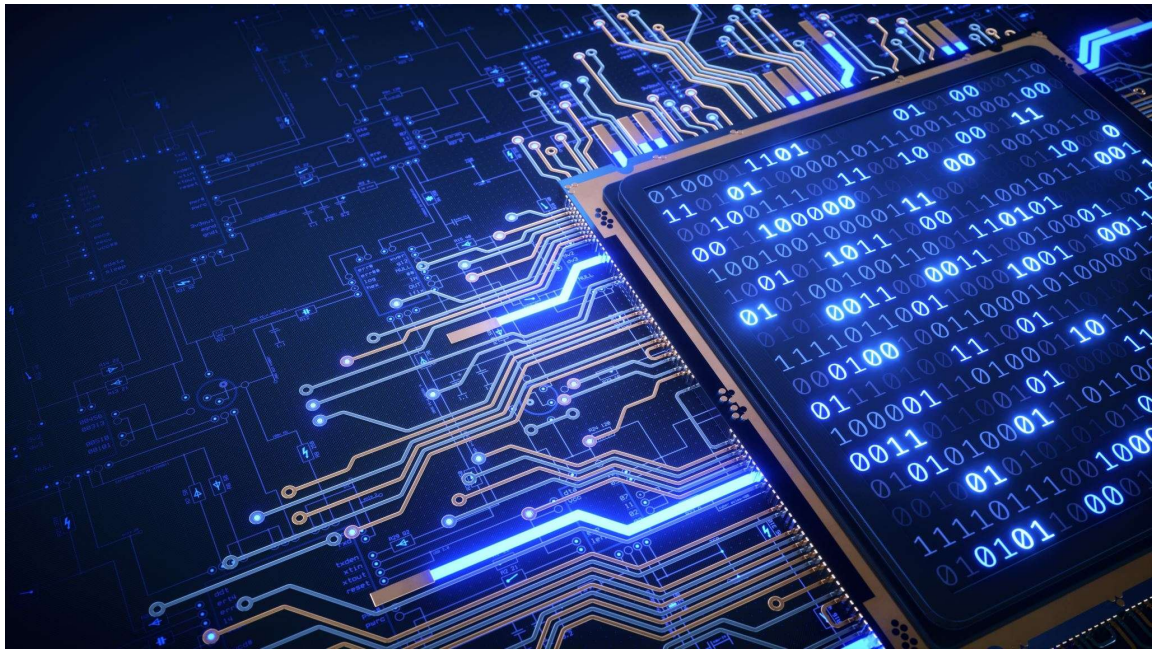
- Primarily based on the two previously existing international standards:
  - ISO/IEC 19790:2012 “Security Requirements for Cryptographic Modules”
  - ISO 24759:2017 “Test Requirements for Cryptographic Modules”

FIPS 140-3 (continued)

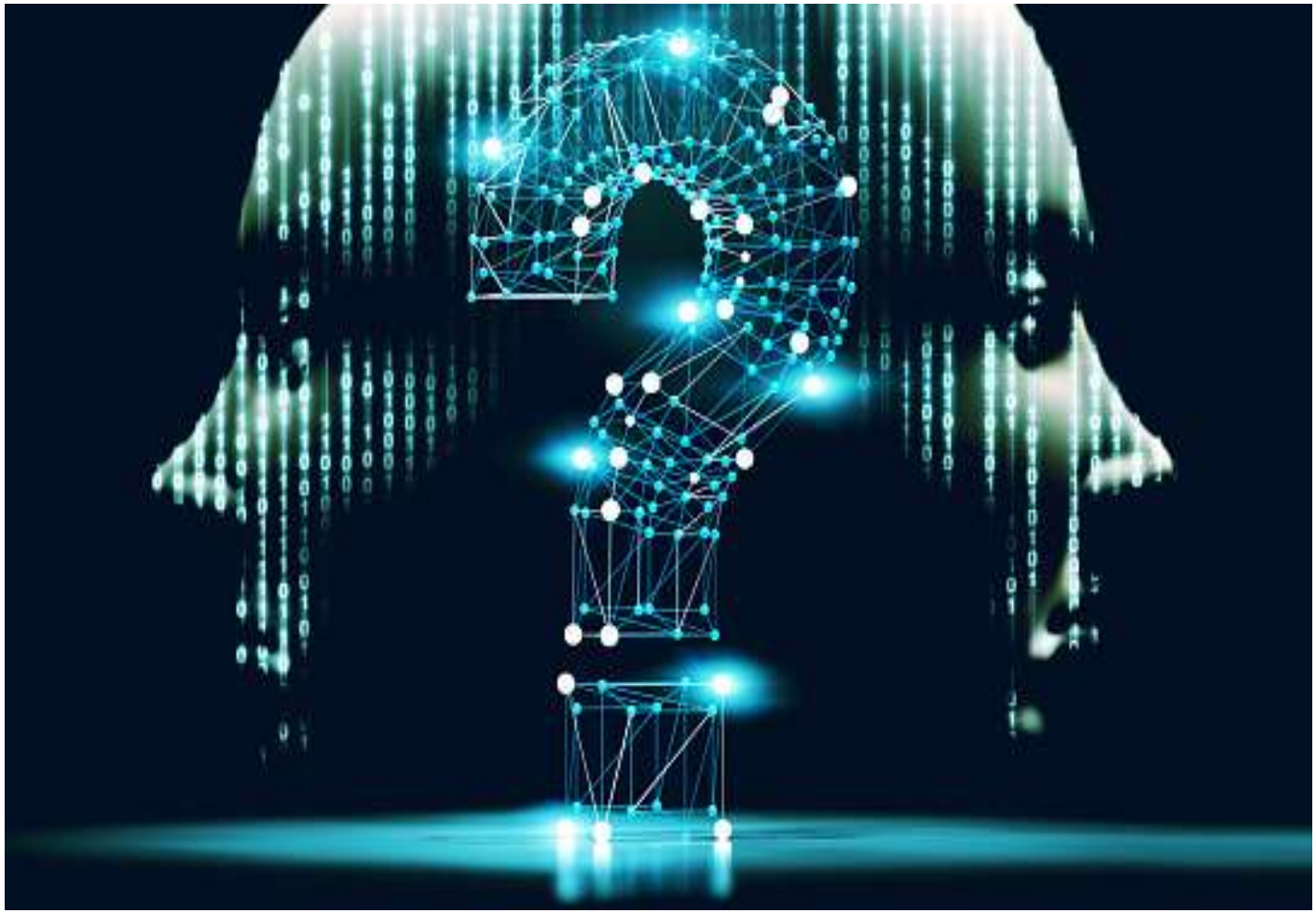
- Level 4 now requires Multi-factor Authentication (MFA)
- Uses Conditional Algorithm Self-Test (CAST) as part of the validation process for cryptographic modules, ensuring algorithms are working correctly before use.
- Allow for the inclusion of Post-Quantum Cryptography (PQC) algorithms

The Quantum Cryptography Paradox

- Encryption will get broken.
- Encryption will get better.
- It is based on the naturally occurring and immutable laws of quantum mechanics.



Questions



Informational Slides

NC DHHS Privacy and Security Policies :
https://policies.ncdhhs.gov/departmental/policies-manuals/section-viii-privacy-and-security/

NC State Security Standards:
https://it.nc.gov/programs/cybersecurity-risk-management/esrmo-initiatives/statewide-information-security-policies

The DHHS Privacy and Security Awareness Hub (Information and Training):
https://www.ncdhhs.gov/about/administrative-offices/privacy-and-security/dhhs-privacy-and-security-awareness-hub

DIT Artificial Intelligence Resource Page:
https://it.nc.gov/resources/artificial-intelligence

Next Meeting Planned for August 14, 2025