Internet Society
Armenia Chapter

Encryption
in
E-Government
&
Digital Governance

Yeghisabet Alaverdyan

Head of Systems Integration Department
EKENG CJSC
PhD

Yerevan, 04.10.2024

Agenda

- E-Government
- Digital Governance
- Fundamentals of Encryption
- Encryption equipped E-Gov
- Key takeaways

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.

E-Government

1. Government-to-Citizen (G2C):

Citizens get access a wide range of services online: *applying for permits, paying taxes, or receiving social benefits. It enhances convenience, transparency, and citizen engagement while reducing bureaucracy.*

2. Government-to-Business (G2B):

Simplifies business interactions with the government: sending and receiving docs digitally, saving time.

3. Government-to-Government (G2G):

Allows for the secure sharing of information and resources, streamlining inter-departmental processes and improving decision-making, offers better collaboration between different government agencies.

4. Government-to-Employee (G2E):

*Automates processes, such as: **customer service**, **data analysis**, **training**, **communication**,*

*and **enhances operational efficiency**. The future is embedding Digital Workers.*

Digital Governance

- is about leveraging digital technology to make government services
  - more efficient,
  - transparent,
  - accessible, and
  - responsive to the needs of the public,

  improving the overall governance process.

Key Components:

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.

It goes beyond simply implementing technology to deliver services.

- refers to the use of digital technologies by governments and organizations to
  - manage,
  - regulate, and
  - enhance
    - ✓ decision-making,
    - ✓ public services, and
    - ✓ societal interactions.

It implements the digital transformation of both public and private sector functions.

Key Aspects:

Policy Frameworks for Digital Transformation: *DG sets the legal and policy guidelines that regulate how digital technologies are integrated into government services, businesses, and social systems.*

Data Intelligence and Governance: *Involves policies and strategies for data protection, privacy, ownership, and access. Governments must ensure that citizens' personal data is handled securely, and that public data is used transparently and ethically.*

Cybersecurity Governance: *Includes creating frameworks for managing risks, responding to cyberattacks, and securing government systems, critical infrastructures, and digital services from APT threats.*

Digital Rights and Inclusivity: 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, and
- safeguarding users from online harassment or surveillance.

Other Key Aspects:

Digital Public Services: *DG involves the use of technology to deliver public services efficiently.*

Regulation of Emerging Technologies: DG *sets the rules for how AI, ML, Blockchain, and Big Data Analytics are used in*

- ✓ **improving governance,**
- ✓ **predicting governance needs,**
- ✓ **automating processes and**
- ✓ **establishing standards to prevent misuse.**

What are differences between E-Governance and Digital Governance?

E-Gov and DG are related but distinct concepts.

E-Gov is about implementing technology in government services,

while

DG 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!

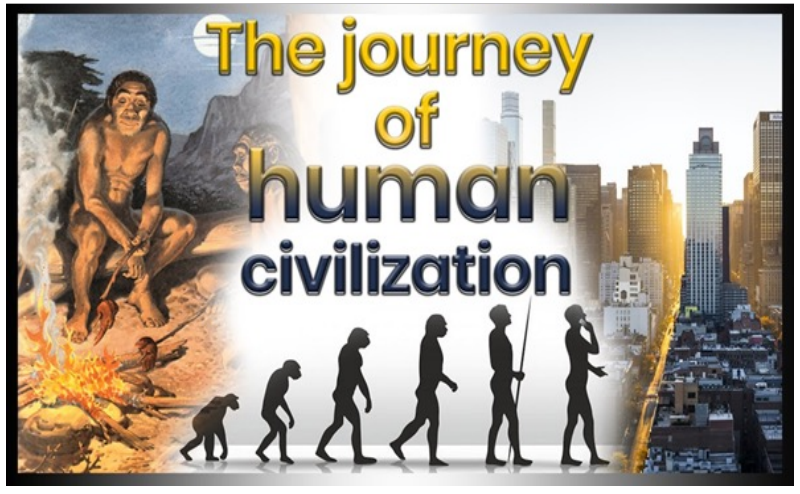
Encryption in E-Government

- E-Gov services handle vast amounts of sensitive data, from personal identification to financial records.
- Encryption is a foundational tool that protects data from unauthorized access, breaches, and tampering.

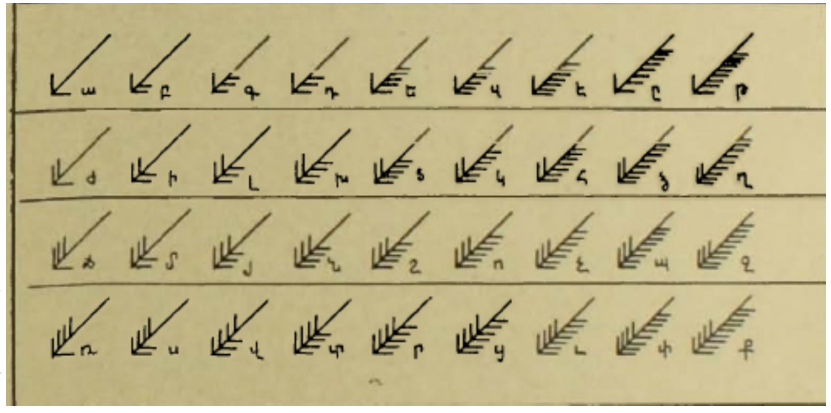
Cryptography & Steganography

Secret Writing

History of Encryption



0.	0..	0...	0....	0.....	0.....	0.....	0.....	0.....
Ա	Բ	Գ	Դ	Ե	Զ	Է	Ը	Թ
00.	00..	00...	00....	00.....	00.....	00.....	00.....	
Ժ	Ի	Լ	Խ	Ծ	Կ	Հ	Ձ	

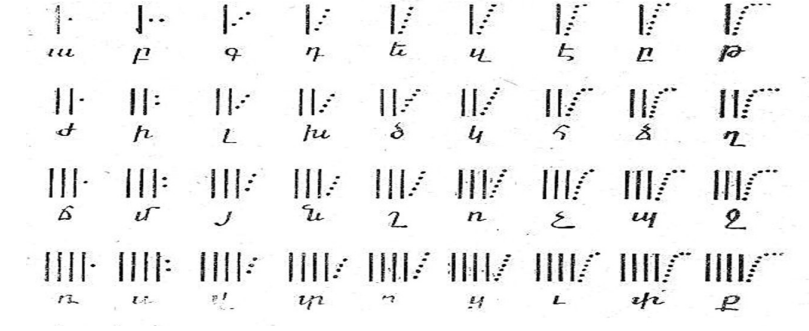


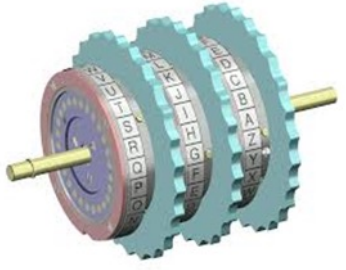
0	ԱԱ	ԱԲ	ԲԲ	ԲԳ	ԳԳ	ԳԴ	ԴԴ	ԴԵ
Ա	Բ	Գ	Դ	Ե	Զ	Է	Ը	Թ
1	2	3	4	5	6	7	8	9

ԵԵ	ԺԺ	ԺԵԺԵ	ԻԻ	ԻԵԻԵ	ԼԼ	ԼԵԼԵ	ԽԽ	ԽԵԽԵ
Ժ	Ի	Լ	Խ	Ծ	Կ	Հ	Ձ	Ղ
10	20	30	40	50	60	70	80	90

ԾԾ	ՃՃ	ՃԾՃԾ	ՄՄ	ՄԾՄԾ	ՅՅ	ՅԾՅԾ	ՆՆ	ՆԾՆԾ
Ճ	Մ	Յ	Ն	Շ	Ո	Չ	Պ	Ջ
100	200	300	400	500	600	700	800	900

ՇՇ	ՌՌ	ՌՇՌՇ	ՍՍ	ՍՇՍՇ	ՎՎ	ՎՇՎՇ	ՏՏ	ՏՇՏՇ
Ռ	Ս	Վ	Տ	Ր	Ց	ՈՒ	Փ	Ք
1000	2000	3000	4000	5000	6000	7000	8000	9000





MODERN CRYPTOGRAPHY IS ALL ABOUT MATH!

Usage of Modern Cryptography

Basic cryptographic principles:

- Symmetric and Asymmetric encryption,
- Hashing
- Digital Signatures

+

Data

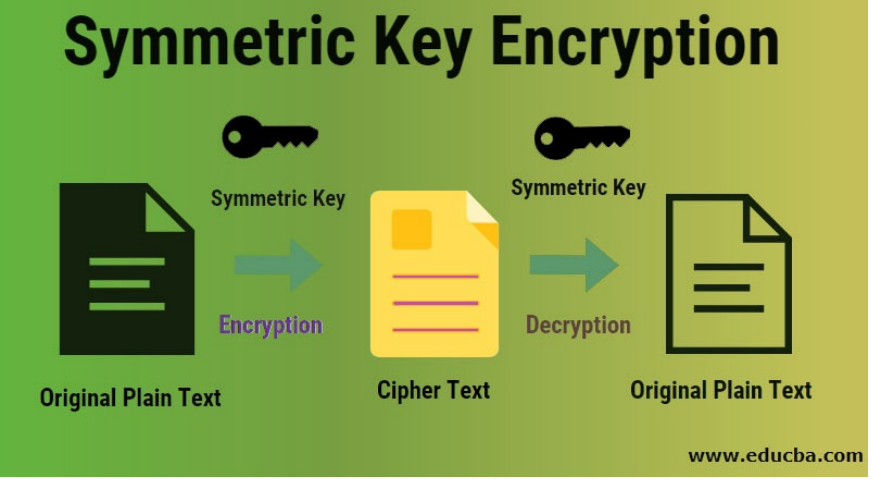
- masking
- anonymization
- randomization
- pseudonymization

All cryptographic protocols should embody these two properties:

confusion

and

diffusion



Symmetric Encryption

REMEDY:
ZERO TRUST MINDSET

Who will ensure?

- uses the same key for both encryption and decryption
- utilizes solely bitwise operations
- is fast

but key management is complex

- Trust Problem
- Key Exchange Problem
- Key Management Problem at large scale

„WENN ZWEI DAS GEHEIMNIS KENNEN, WISSEN DIE SCHWEINE

The ZERO-TRUST Approach

Zero-trust is not a technology, but rather a philosophy, a way of thinking…

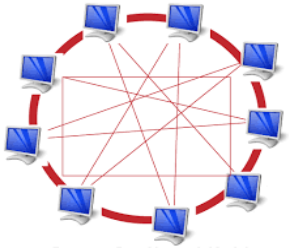
John Kindervag, 2010.

Trust no one or anything — and always verify VS **Trust, but verify**

Confidential Computing

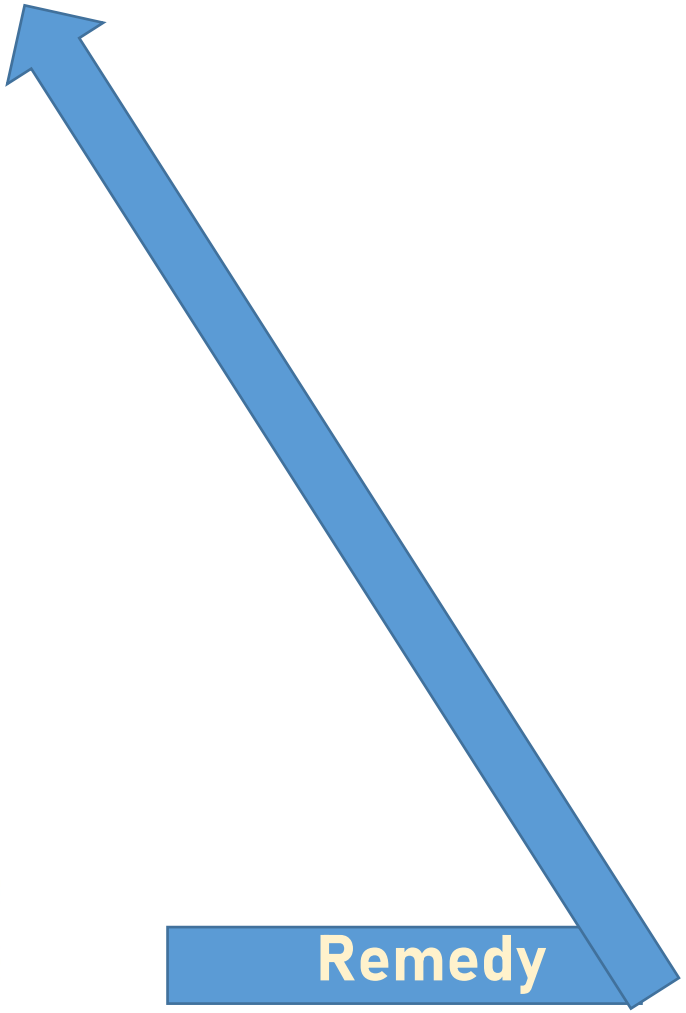
The three states of data

Data at rest: encryption helps



Data in transit: encryption helps

Data in use: encryption does not help



Homomorphic Encryption

Confidential Computing Paradigm

CC

- ✓ **protects data in use** by isolating data and performing computations in a hardware-based Trusted Execution Environment (TEE), **a secure part of the processor.**
- ✓ **HSM**

- ✓ **removes** a number of entities – such as:
  - ✓ the operating system,
  - ✓ device drivers,
  - ✓ cloud providers,
  - ✓ admins,
  - ✓ data owners, and even
  - ✓ the programmers.

ZT & CC Mathematical Models In E-Gov

Strongly recommended:

- Zero-knowledge proof of identity
- Non-transferable digital signatures
- Biometric data remote verification and liveness check **(AI/ML tools)**
- Digital signatures in Ad Hoc Networks: membership verification
- Group Signatures
- Bit commitment
- Esoteric protocols
- Threshold Cryptography
- Verifiable secret splitting
- Verifiable secret sharing
- Multi-party computation equipped with verifiable secret sharing

Zero Knowledge Proofs of Identity in E-GOV

ZK

- enables specific actions that can be completed without sacrificing valuable secret or identifying information.

Users' identity can be strictly verified by

- ✓ performing some identification protocol related to its public key, f.e. by demonstrating knowledge of a modular square root of this key,
- ✓ proving associated isomorphism between a pair of graphs,
- ✓ proving statements phrased as Boolean circuits, based on garbled circuits,
- ✓ computing (Canonical) Disjunctive normal forms for a large Boolean circuits,
- ✓ implementing non-transferable confidence,
- ✓ embedding SRP6 protocol, etc…

Stream ciphers vs block ciphers

Modern Symmetric Ciphers

AES (Advanced Encryption Standard), the most widely adopted : *widely used symmetric encryption standard adopted by the U.S. government in 2001. It supports key sizes of 128, 192, and 256 bits.*
Five modes of operation of the AES algorithm were standardized: ECB (Electronic Code Book), CBC (Cipher Block Chaining), CFB (Cipher Feedback), OFB (Output Feedback) and CTR (Counter).

GCM (Galois/Counter Mode): *is not a standalone cipher but a mode of operation for block ciphers (like AES) that provides authenticated encryption., combines encryption and integrity verification.*

Blowfish: *created by Bruce Schneier in 1993, is a fast block cipher that uses variable-length keys (from 32 to 448 bits). It's designed to replace DES.*

Twofish: *successor to Blowfish, also designed by Bruce Schneier. It supports key sizes of up to 256 bits and is known for its speed and security.*

Modern Symmetric Ciphers

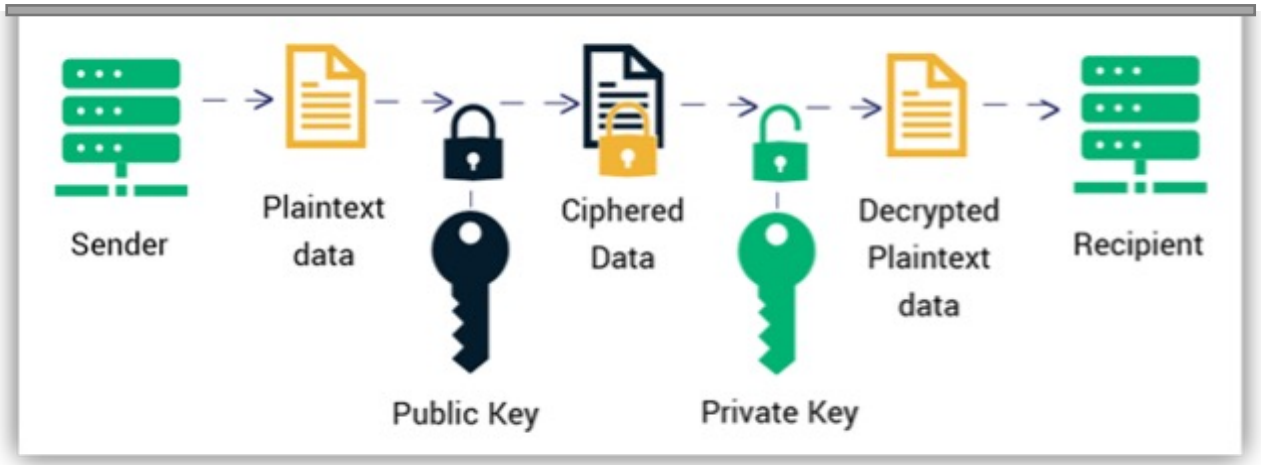
Serpent: *block cipher that was a finalist in the AES competition. It supports key sizes of 128, 192, and 256 bits, emphasizing a high level of security.*

RC4: *stream cipher designed by Ron Rivest. While it was widely used in protocols like SSL/TLS, vulnerabilities have been discovered, making it less secure for modern use.*

Salsa20: *stream cipher developed by Daniel J. Bernstein that expands a 256-bit key into 2^64 randomly accessible streams, each containing 2^64 randomly accessible 64-byte (512 bits) blocks*

ChaCha20: *stream cipher designed by Daniel Bernstein as a variant of Salsa20. It provides high performance and security with a 256-bit key size.*

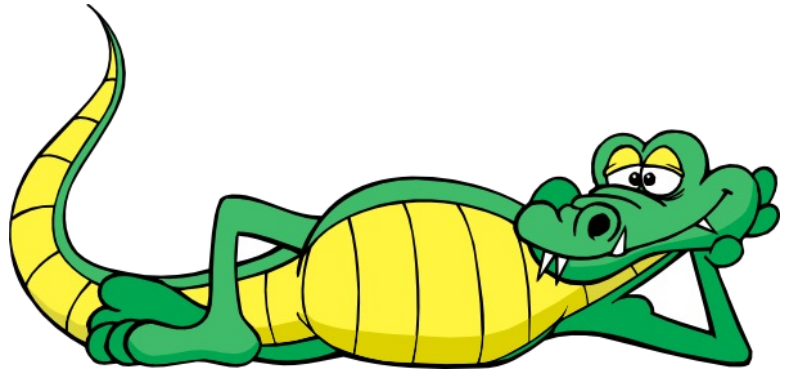
XChaCha20: *an extension of ChaCha20, XChaCha20 adds an extended nonce size for better security against nonce reuse. It also retains the same performance benefits as ChaCha20.*

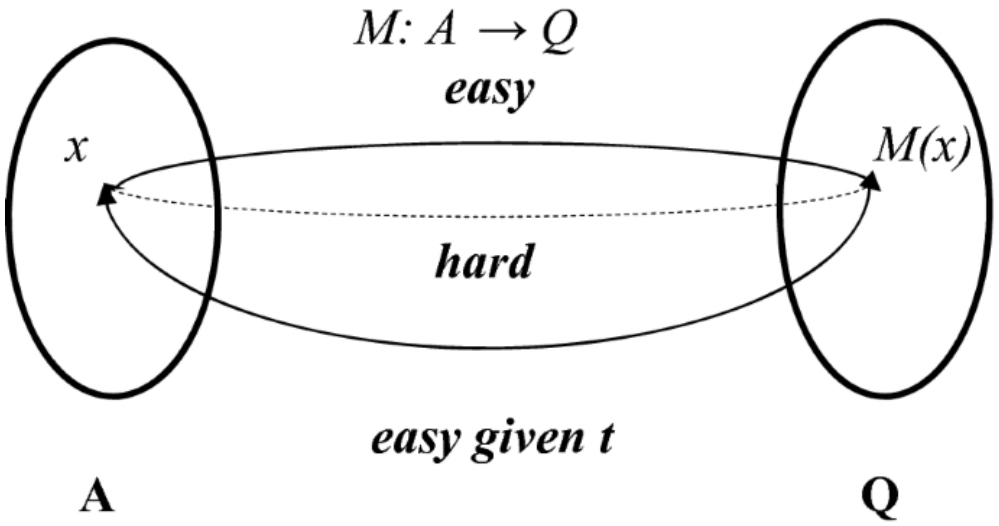


Asymmetric Encryption

Opens new opportunities…

- Uses a public-private key pair
- Eliminates the Key Exchange Problem
- Is computationally more demanding
  - involves a suitable Trapdoor one-way function





Cryptographic Trap-door One-way functions

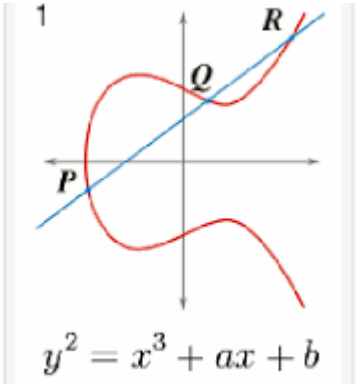
- **Factoring the product of two large prime numbers**. Given a public key (the product of two primes), it's easy to compute the function, but without the private key (the two primes), it's computationally hard to reverse it.
- **Discrete logarithm problem**, which is difficult to reverse without a secret key.
- **Computing discrete logarithms in a finite field.**
- **Lattice-based** *(RAST binary Relation based)* **cryptographic system** that relies on the difficulty of certain mathematical problems in polynomial rings.

Asymmetric Cryptography Algorithms

RSA (Rivest–Shamir–Adleman): *one of the oldest and most widely used asymmetric ciphers. It relies on the mathematical difficulty of factoring large composite numbers.*

1: **Input Values:** p and q
2: **Compute:**
3: n = p x q
4: (n) = (p-1) (q-1)
5: **Select Integer values:** e [(gcd (), e) - 1; 1 < e < ϕ (n)]
6: **Compute:** d de *mod* ϕ (n) = 1
7: C = Cg 1 *mod* (z)
8: **Encryption:** M < n C = M (*mod* n)
9: **Decryption:** CM = C(*mod* n)

Elliptic Curve Cryptography (ECC):
uses the mathematics of elliptic curves over finite fields to create smaller, yet highly secure keys compared to RSA. This results in faster computations and lower power consumption.



Prime field vs Binary field

Diffie-Hellman Key Exchange:
While primarily a key exchange protocol,
Diffie-Hellman can be considered a form of asymmetric cryptography.
It allows two parties to securely share a secret key over an insecure channel.

Asymmetric Cryptography Algorithms

DSA (Digital Signature Algorithm): *used for digital signatures, ensuring data integrity and authenticity. It relies on the discrete logarithm problem.*

ElGamal Encryption: *is based on the difficulty of the discrete logarithm problem.*

Post-Quantum Cryptography: *research is ongoing to develop asymmetric ciphers that are resistant to quantum attacks. Examples include:*

- ***Lattice-based Cryptography (e.g., NTRU)**: Based on hard lattice problems.*
- ***Code-based Cryptography (e.g., McEliece)**: Based on the difficulty of decoding random linear codes.*
- ***Multivariate Quadratic Equations (MQ)**: Involves solving systems of multivariate polynomial equations.*

Hybrid Cryptosystems: *is the combination of asymmetric and symmetric encryption, where asymmetric ciphers are used to securely exchange symmetric keys.*

Other

of

Asymmetric Encryption Techniques

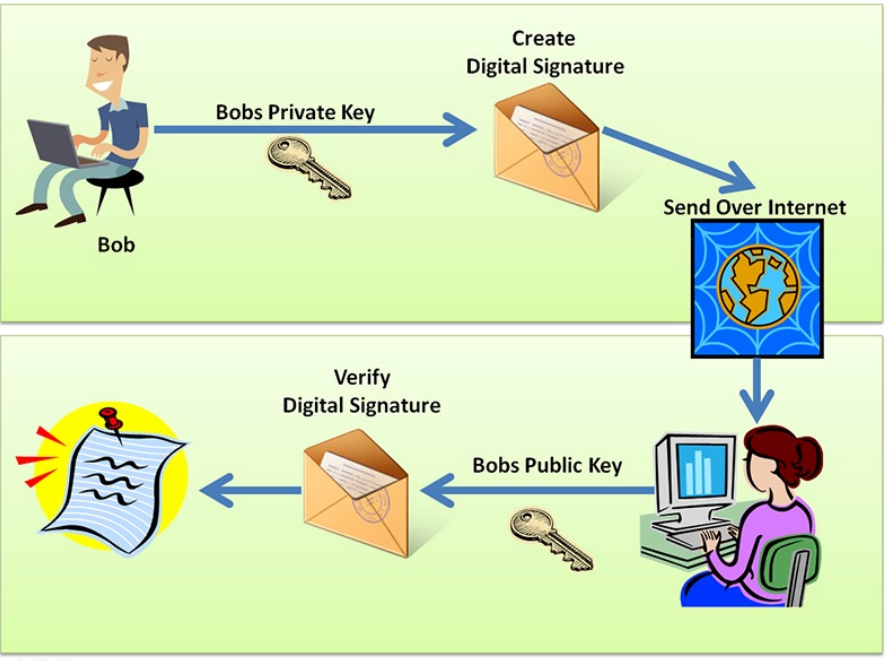
Public Key Infrastructure (PKI) in Digital Governance

IAAA: **Identification +** **MF Authentication** **+Authorization + Accountability**

What you know
What you have
Who you are

- **Management of digital certificates and public keys in a secure way**
- **Provision of**
  - secure digital identities,
  - authentication, and
  - encrypted communications

  in E-Government platforms.



Digital Signatures and Authentication

1. **The signature is authentic.** *The signature convinces the document's recipient that the signer deliberately signed the document.*
2. **The signature is unforgeable.** *The signature is proof that the signer, and no one else, deliberately signed the document.*

3. **The signature is not reusable.** *The signature is part of the document; an unscrupulous person cannot move the signature to a different document.*

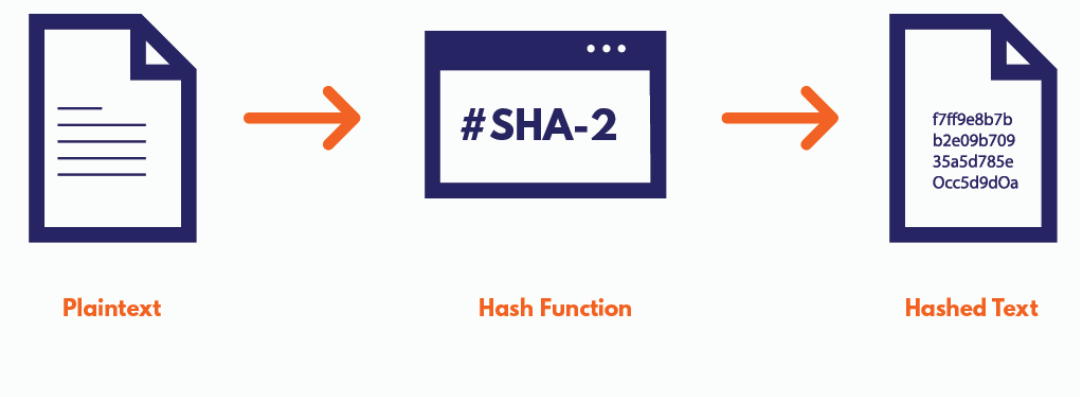
4. **The signed document is unalterable.** *After the document is signed, it cannot be altered.*
5. **The signature cannot be repudiated.** *The signature and the document are physical things. The signer cannot later claim that he or she didn't sign it.*

Blockchain and Encryption in E-Government

Blockchain, with its decentralized, immutable ledger, is increasingly being integrated into digital governance to enhance transparency and security.

Encryption plays a critical role in securing Blockchain transactions and ensuring that sensitive information is protected.

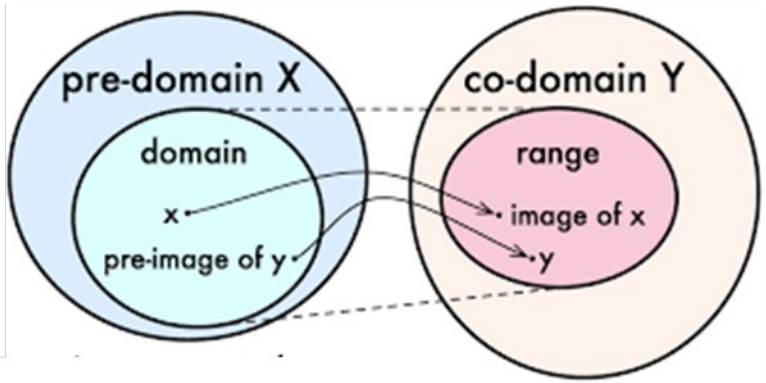
Hash Functions



❖are used

- ➢ to convert information to a **fixed size length**
- ➢ in cryptocurrency to secure Blockchain information

Should be Pre-image resistant!

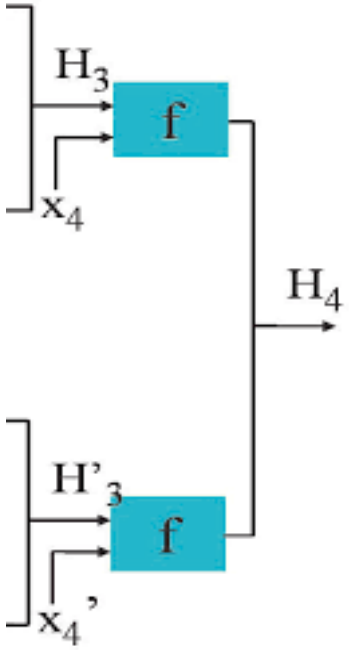


Cryptographic Hash Function

Stop identity spoofing

SHOULD BE:

- **collision resistant**
- **second pre-image resistant**



- Encryption is a foundational element that strengthens trust, security, and efficiency in digital governance, ultimately leading to more effective and resilient E-GOV operations.

Data Privacy and Security: This fosters trust between citizens and institutions, crucial for effective governance.
Integrity of Information: This is important for maintaining the integrity of records and communications.
Secure Communication: Encrypted channels allow secure communication between government officials and agencies.
Regulatory Compliance: Encryption helps governments comply with laws like GDPR.

Facilitating E-Governance: Encryption ensures secure transactions and interactions. This encourages greater citizen participation in digital governance.
Protection Against Cyber Threats: Strong encryption and MFA can mitigate the insider/outsider risks, safeguarding critical infrastructure and services.
Empowering Citizens: By securing personal data, encryption empowers citizens to engage with digital platforms without fear, enhancing public participation and transparency in governance.


Thank you !