Cryptography Classes in Bugs Framework (BF):
Encryption Bugs (ENC), Verification Bugs (VRF), and Key Management Bugs (KMN)

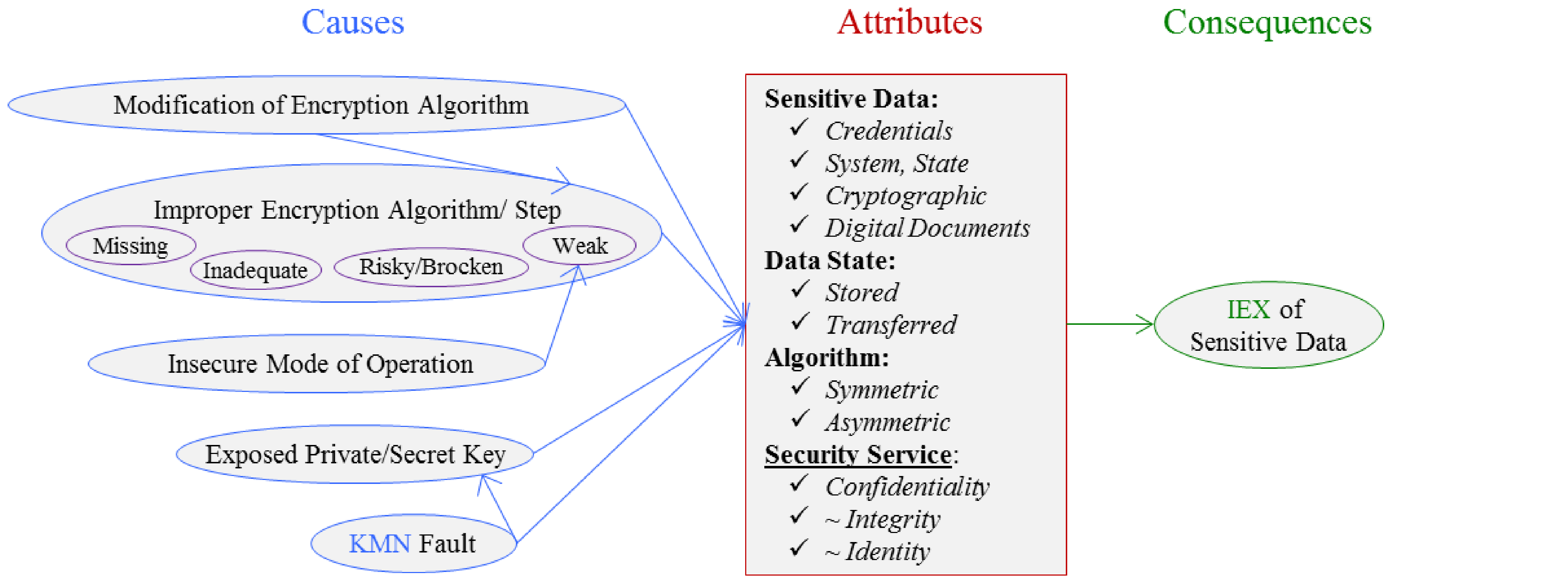
Irena Bojanova, NIST; Paul E. Black, NIST; Yaacov Yesha, NIST, UMBC; Farhan Nadeem, NIST

Advances in scientific foundations of cybersecurity rely on the availability of accurate, precise, and unambiguous definitions of software weaknesses (bugs) and clear descriptions of software vulnerabilities.
The Bugs Framework (BF) comprises rigorous definitions and (static) attributes of bug classes, along with their related dynamic properties, such as proximate, secondary and tertiary causes, consequences, and sites.

BF Taxonomy

Encryption Bugs (ENC): *The software does not properly transform sensitive data (plaintext) into unintelligible form (ciphertext) using cryptographic algorithm and key(s).*

Decryption Bugs: The software does not properly transform ciphertext into plaintext using cryptographic algorithm and key(s).



Causes

- Modification of Encryption Algorithm
- Improper Encryption Algorithm/ Step: Missing, Inadequate, Risky/Brocken, Weak
- Insecure Mode of Operation
- Exposed Private/Secret Key
- KMN Fault

Attributes

Sensitive Data:
- ✓ *Credentials*
- ✓ *System, State*
- ✓ *Cryptographic*
- ✓ *Digital Documents*

Data State:
- ✓ *Stored*
- ✓ *Transferred*

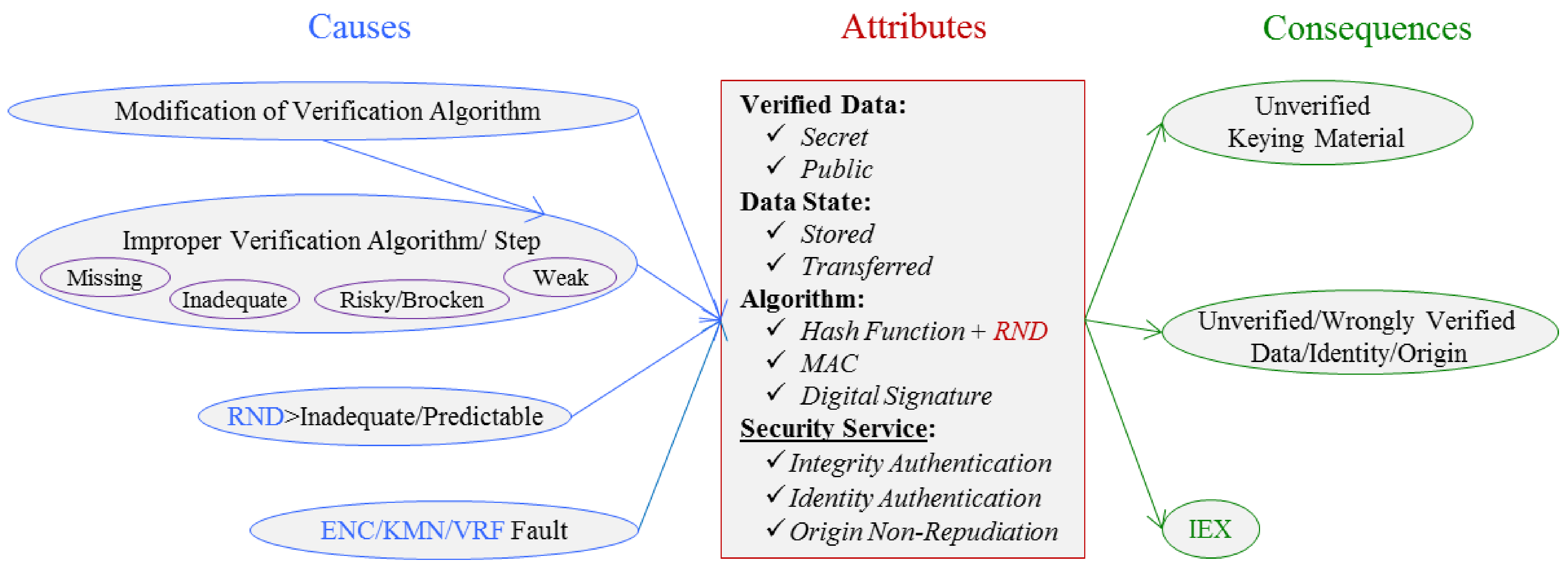
Algorithm:
- ✓ *Symmetric*
- ✓ *Asymmetric*

Security Service:
- ✓ *Confidentiality*
- ✓ *~ Integrity*
- ✓ *~ Identity*

Consequences

- IEX of Sensitive Data

Verification Bugs (VRF): *The software does not properly sign data, check and prove source, or assure data is not altered.*



Causes

- Modification of Verification Algorithm
- Improper Verification Algorithm/ Step: Missing, Inadequate, Risky/Brocken, Weak
- RND>Inadequate/Predictable
- ENC/KMN/VRF Fault

Attributes

Verified Data:
- ✓ *Secret*
- ✓ *Public*

Data State:
- ✓ *Stored*
- ✓ *Transferred*

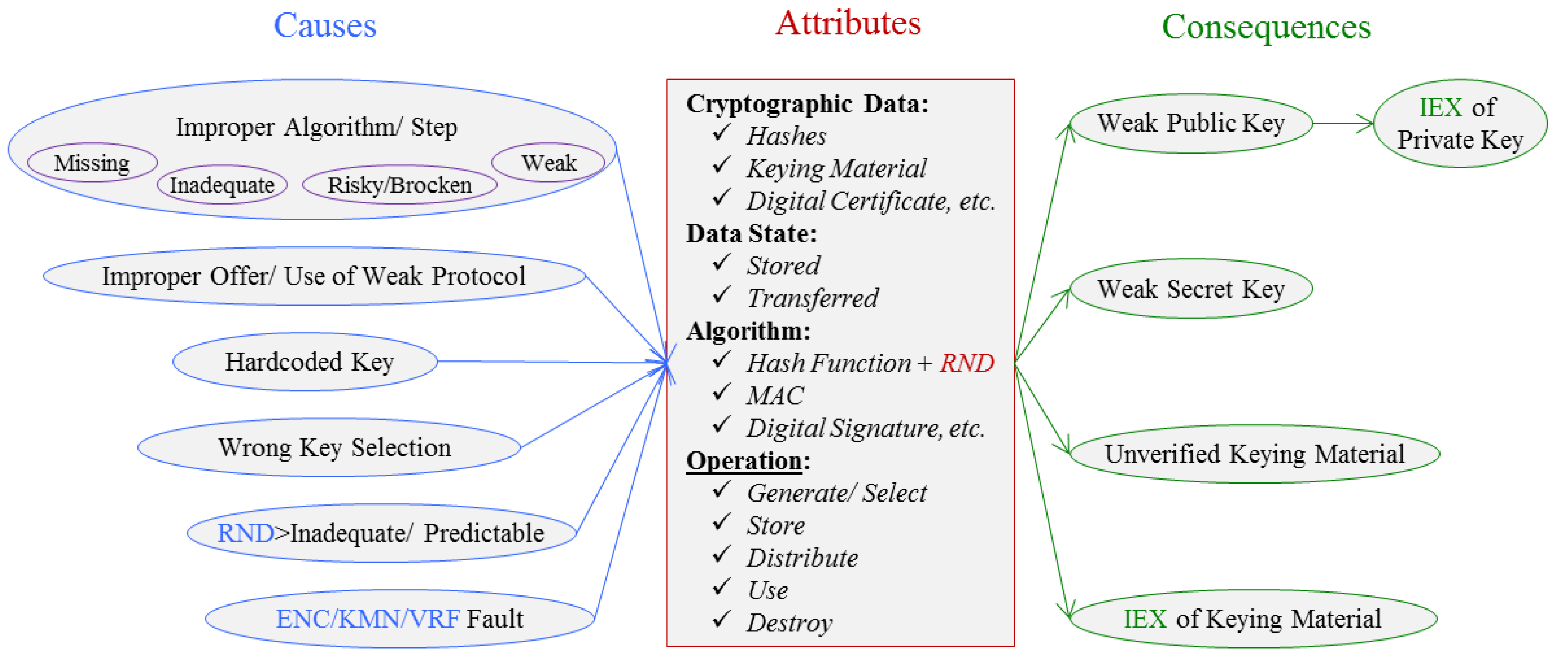
Algorithm:
- ✓ *Hash Function + RND*
- ✓ *MAC*
- ✓ *Digital Signature*

Security Service:
- ✓ *Integrity Authentication*
- ✓ *Identity Authentication*
- ✓ *Origin Non-Repudiation*

Consequences

- Unverified Keying Material
- Unverified/Wrongly Verified Data/Identity/Origin
- IEX

Key Management Bugs (KMN): *The software does not properly generate, store, distribute, use, or destroy cryptographic keys and other keying material.*



Causes

- Improper Algorithm/ Step: Missing, Inadequate, Risky/Brocken, Weak
- Improper Offer/ Use of Weak Protocol
- Hardcoded Key
- Wrong Key Selection
- RND>Inadequate/ Predictable
- ENC/KMN/VRF Fault

Attributes

Cryptographic Data:
- ✓ *Hashes*
- ✓ *Keying Material*
- ✓ *Digital Certificate, etc.*

Data State:
- ✓ *Stored*
- ✓ *Transferred*

Algorithm:
- ✓ *Hash Function + RND*
- ✓ *MAC*
- ✓ *Digital Signature, etc.*

Operation:
- ✓ *Generate/ Select*
- ✓ *Store*
- ✓ *Distribute*
- ✓ *Use*
- ✓ *Destroy*

Consequences

- Weak Public Key → IEX of Private Key
- Weak Secret Key
- Unverified Keying Material
- IEX of Keying Material

Examples

CVE-2007-5460 → ENC
Cause: Weak Encryption Algorithm (XOR cipher with fixed key)
Attributes:
Sensitive Data: Credentials (PINs/passwords)
Data State: Transferred (over network)
Algorithm: Symmetric (that allows obtaining shared key /by sniffing or spoofing the docking process/ and decryption)
Security Service: Confidentiality
Consequence: IEX of Sensitive Data (credentials)

CVE-2002-1697 → ENC
Causes: Insecure Mode of Operation (ECB) leads to Weak Encryption Algorithm (for same shared key produces same ciphertext from same plaintext)
Attributes:
Sensitive Data: Any (Credentials, Cryptographic, …)
Data State: Transferred (over network)
Algorithm: Symmetric (that allows identifying patterns and data recovery)
Security Service: Confidentiality
Consequence: IEX of Sensitive Data

CVE 2001-1585 → VRF
Cause Missing Verification Step (challenge-response) in public key authentication
Attributes:
Verified Data: Any (Secret/ Public)
Data State: Transferred (over network)
Algorithm: Digital Signature (not using such allows private key not to be verified by public key)
Security Service: Identity Authentication
Consequence: IEX

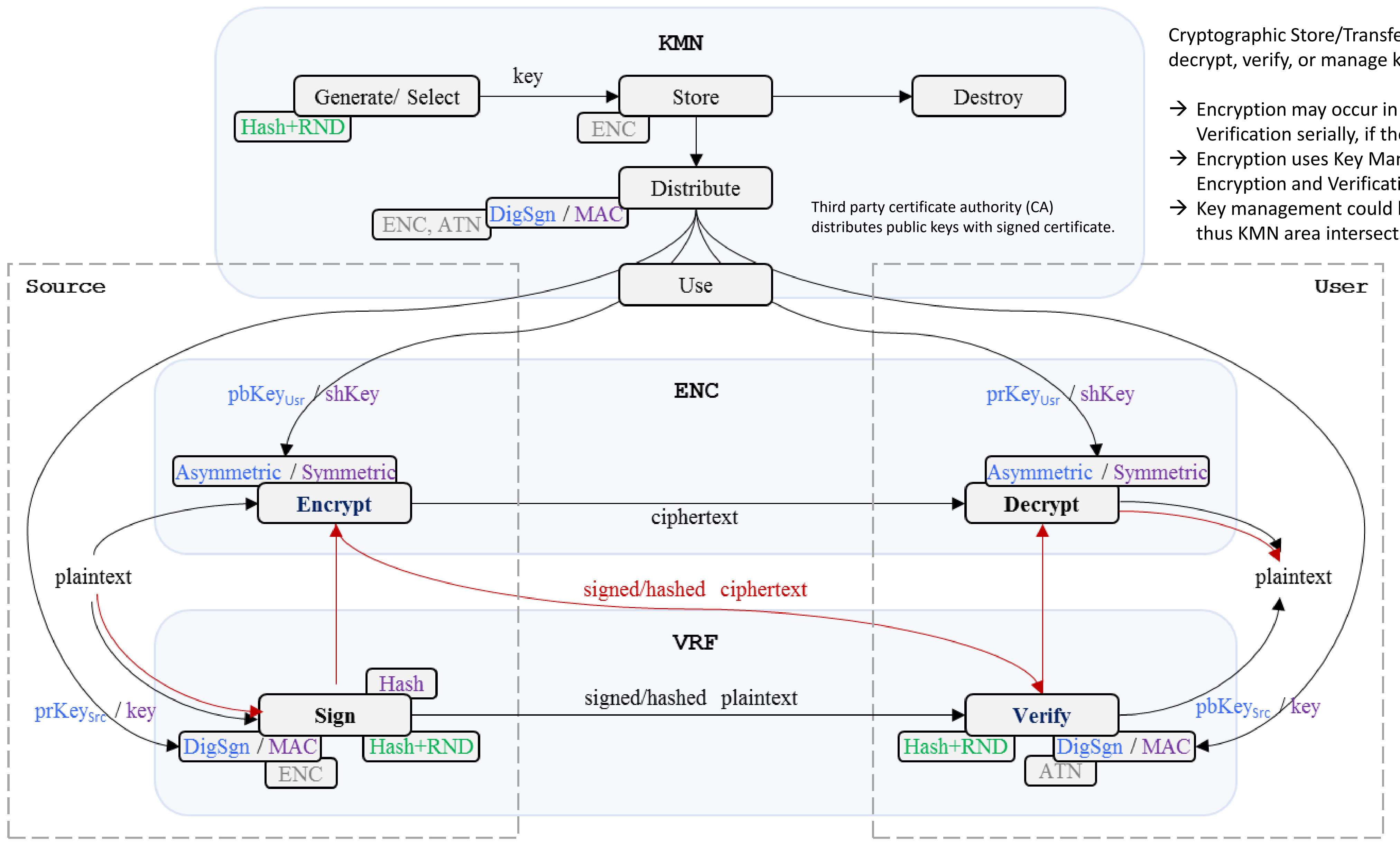
CVE 2015-2141 → VRF
Cause: Modification of Verification Algorithm by adding a step (blinding)
Attributes:
Verified Data: Any (Secret/ Public)
Data State: Transferred (over network)
Algorithm: Digital Signature (Rabin-Williams) (that allows obtaining the private key in cases of incorrect unblinding)
Security Service: Identity Authentication
Consequence: IEX

CVE-2015-0204, 1637, 1067 (FREAK) → KMN & ENC
An inner KMN leads to an inner ENC, which leads to an outer ENC.
Inner KMN:
Cause: Improper Offer of Weak Protocol (Export RSA – offered from MITM-tricked server and accepted by client)
Attributes:
Cryptographic Data: Keying Material (pair of private and public keys)
Data State: Transferred (over network)
Algorithm: Export RSA (512-bits key generation based on prime numbers, such that private key can be obtained from public key through factorization)
Operation: Generate
Consequence: IEX Keying Material (private key)

Inner ENC:
Causes: KMN Fault leads to Exposed Private Key
Attributes:
Sensitive Data: Cryptographic (Pre-Master Secret)
Data State: Transferred (over network)
Algorithm: Asymmetric (RSA) (that allows decryption of Pre-Master Secret using exposed private key and computation of Master Secret)
Security Service: Confidentiality
Consequence: IEX of Sensitive Data (Master Secret)

Outer ENC:
Causes: KMN Fault leads to Exposed Secret Key (Master Secret)
Attributes:
Sensitive Data: Credentials (passwords, credit cards)
Data State: Transferred (over network)
Algorithm: Symmetric (key is known)
Security Service: Confidentiality
Consequence: IEX of Sensitive Data (credentials)

Model of Cryptographic Store or Transfer Bugs



Third party certificate authority (CA) distributes public keys with signed certificate.

Cryptographic Store/Transfer Bugs: The software does not properly encrypt/ decrypt, verify, or manage keys for data to be securely stored or transferred.

→ Encryption may occur in tandem with Verification or it may precede Verification serially, if the cipertext is signed or hashed.
→ Encryption uses Key Management, and Key Management likely uses Encryption and Verification to handle keys.
→ Key management could be by third party, source, or user – thus KMN area intersects Source and User areas.

Symmetric—one secretly shared key shKey
- Source encrypts with shKey
- User decrypts with shKey.

Asymmetric—two related keys (public, private)
Source (pbKey$_{Srs}$, prKey$_{Srs}$)
User (pbKey$_{Usr}$, prKey$_{Usr}$)
- Source encrypts with pbKey$_{Usr,}$
- User decrypts with prKey$_{Usr}$
- Source signs with prKey$_{Srs}$
- User verifies with pbKey$_{Srs}$