RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: **PDAC-W12**

CYBER IS HOT; CRYPTO IS NOT

Sandra Lambert

CEO
Lambert & Associates
X9F4 Workgroup Vice Chair

Jeff Stapleton

VP Security Architect
Wells Fargo
X9F4 Workgroup Chair

Tip of the Iceberg

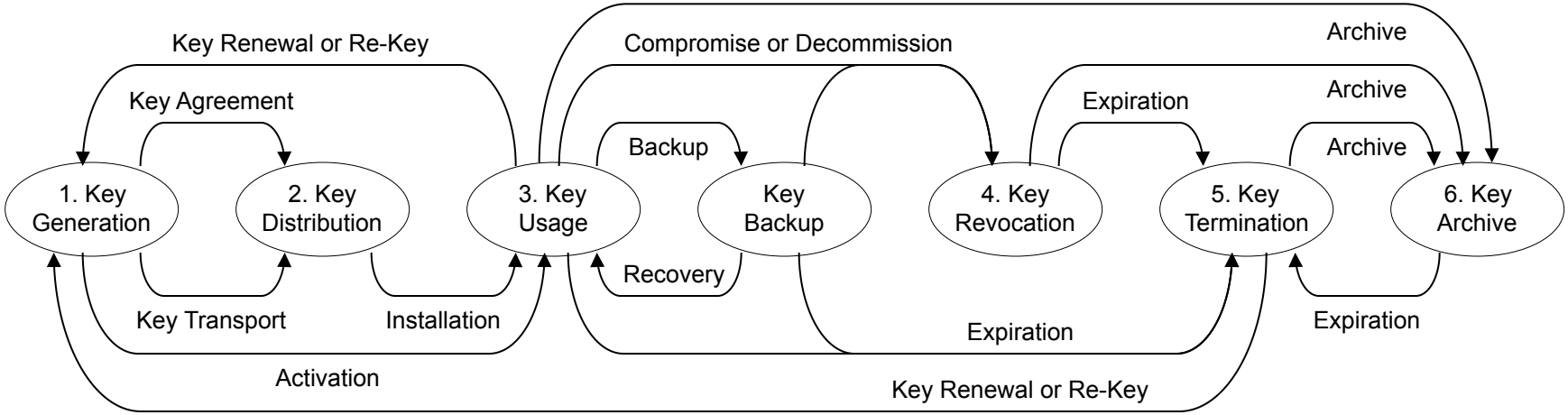
- Introduction
  - What is cybersecurity?
  - What is cryptography?
  - What is key management?
  - How do they work together?
- Problems
- Conclusions

NICCS Definitions

- National Initiative for Cybersecurity Careers and Studies
  - https://niccs.us-cert.gov/glossary
- **Cybersecurity**
  - The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation
- **Cryptography**
  - The use of mathematical techniques to provide security services, such as confidentiality, data integrity, entity authentication, and data origin authentication

ANSI X9.79

- **Key management**
  - Secure administration of the cryptographic key lifecycle



Helping Hands

Crypto secures Cyber

- TLS secures HTTP and others
- IPsec secures IP connections
- SSH secures admin connections
- EMV secures payment cards
- PIN encryption secures cards
- FDE secures laptops
- DBE secures databases
- PSH secures password storage
- PBE secures cryptographic keys

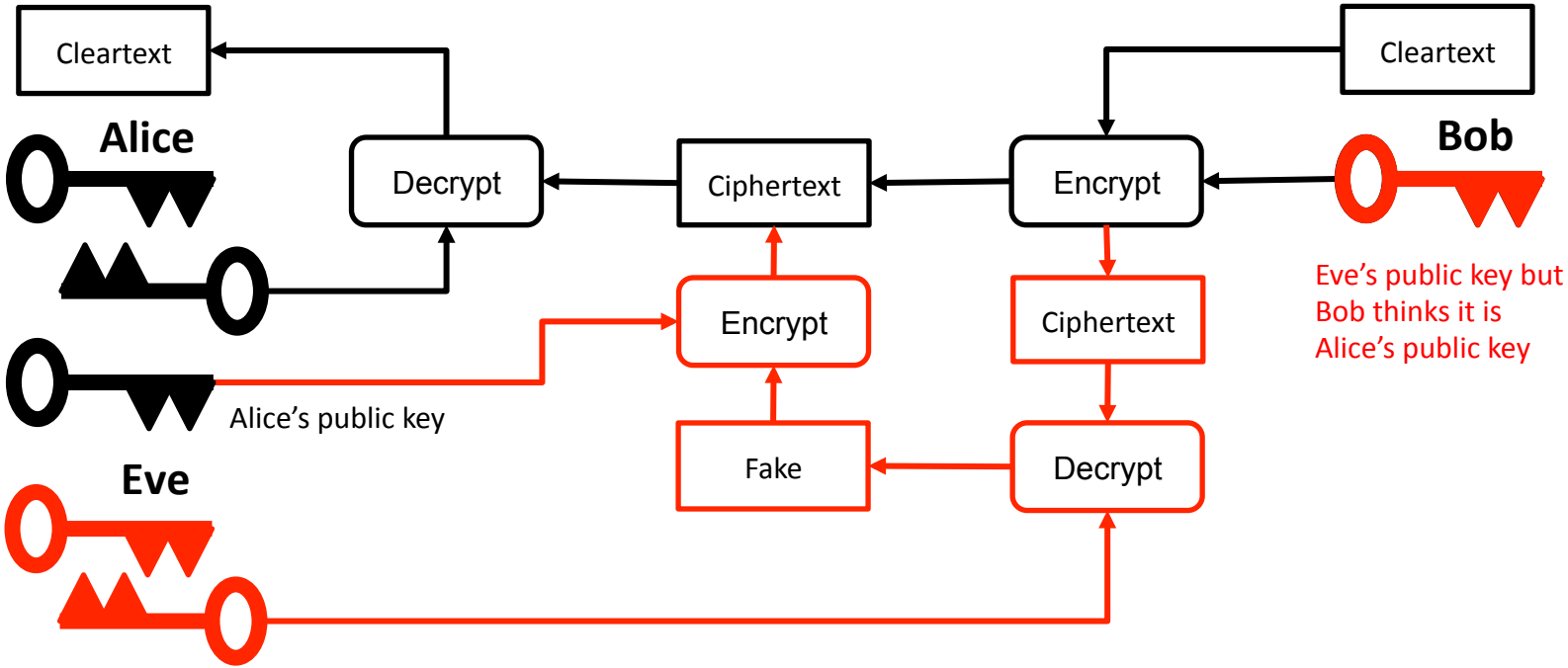
Cyber secures Crypto

- Authentication
  - Passwords
  - Smartcards
  - Biometrics
- Authorization
  - Privileged access
- Accountability
  - Monitoring
  - Logs
  - Analysis

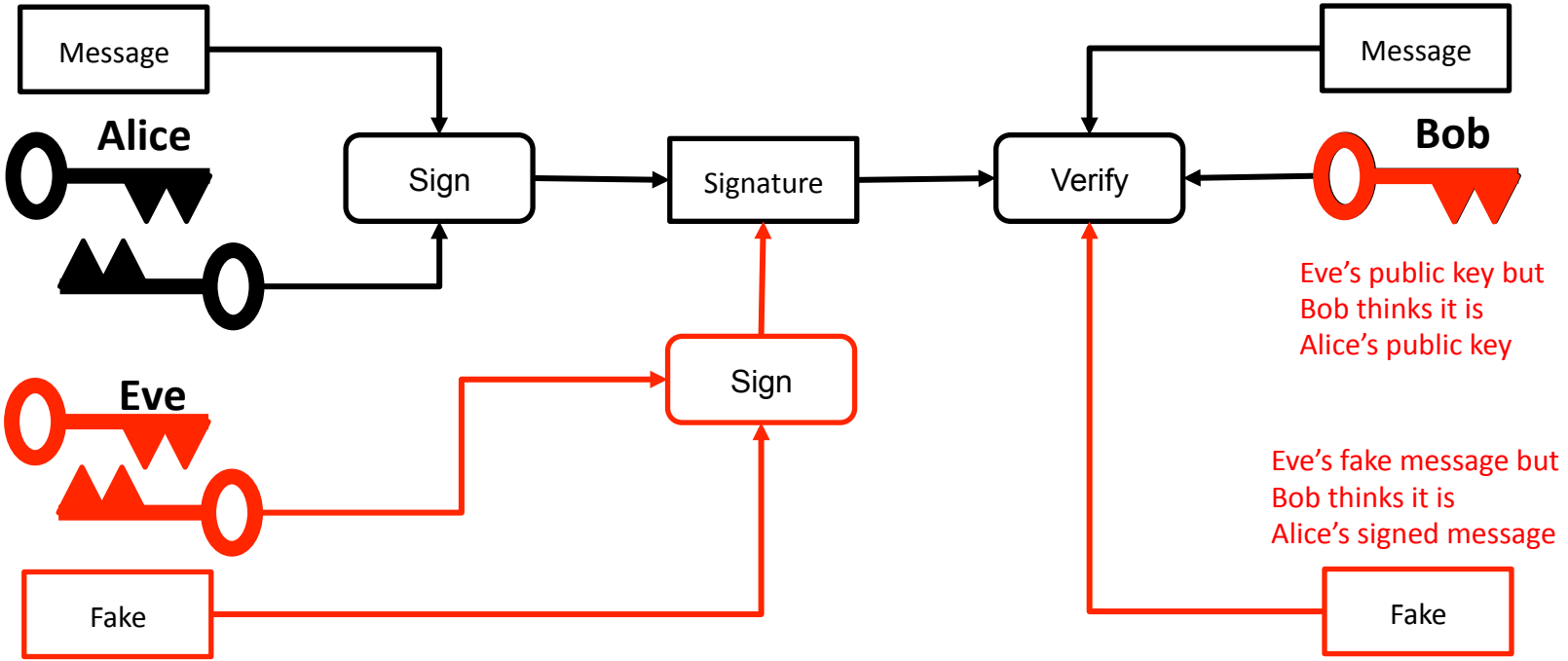
PROBLEMS

What could go wrong?

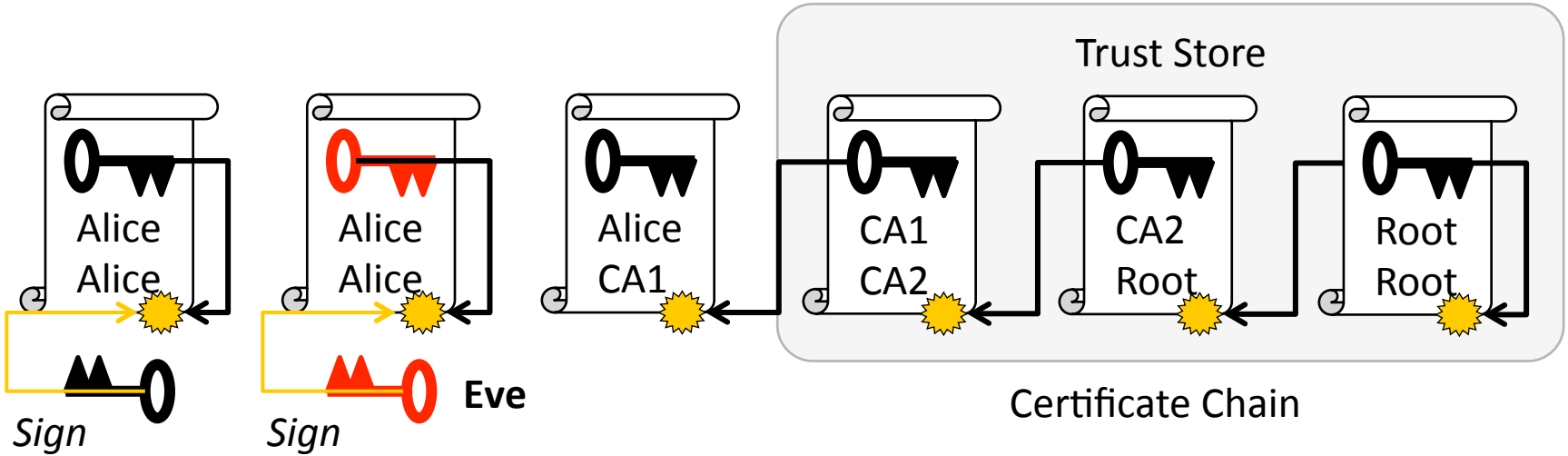
Raw public key: encryption



Raw public key: signature



Self-sign User Certificates



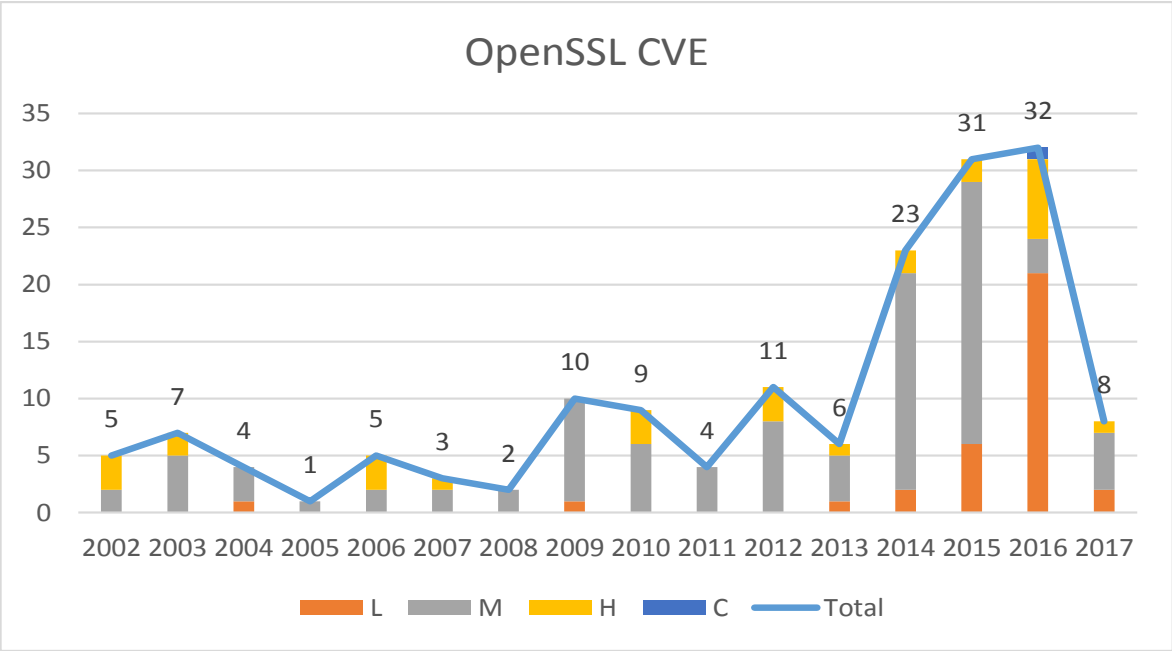
Relying party cannot distinguish between
Alice's self-signed certificate versus
Eve's self-signed certificate

IMPLEMENTATIONS

What else could go wrong?

Case Study: OpenSSL

- Common Vulnerabilities and Exposures (CVE)

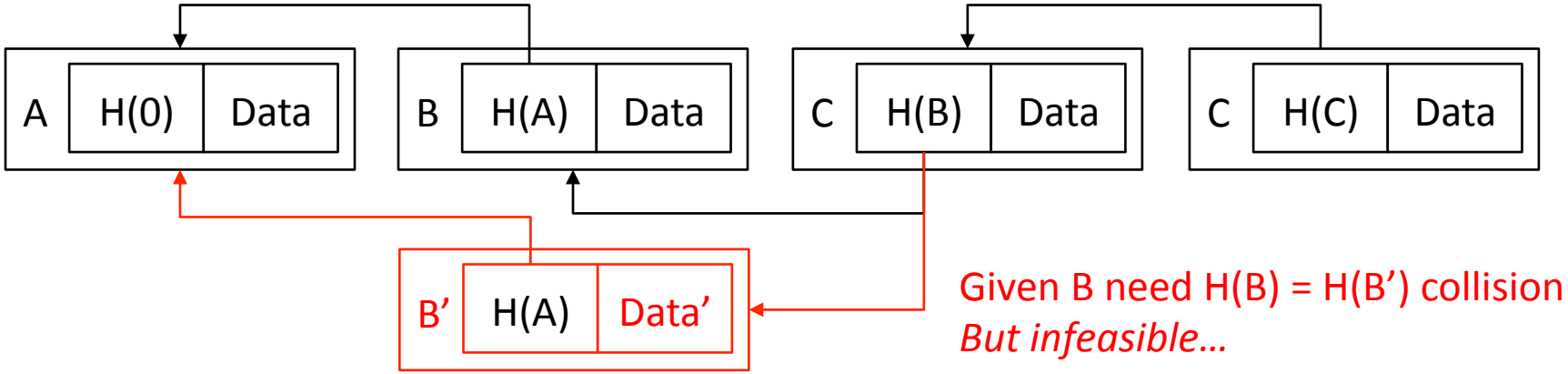


Totals over 16 years

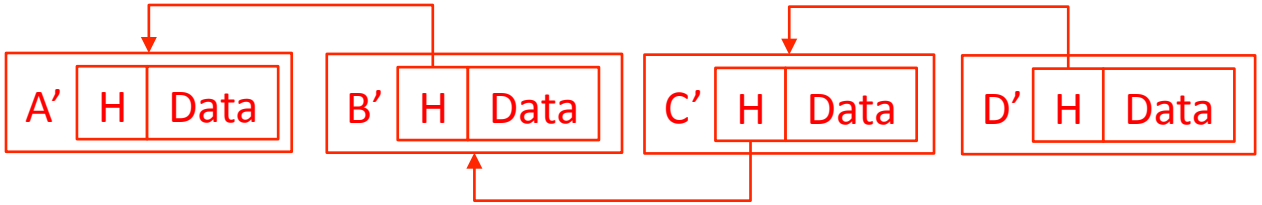
- **161 CVE**
- 34 Low
- 98 Moderate
- 28 High
- 1 Critical

OpenSSL is common cryptographic library
Many others…

Blockchain *Immutability*



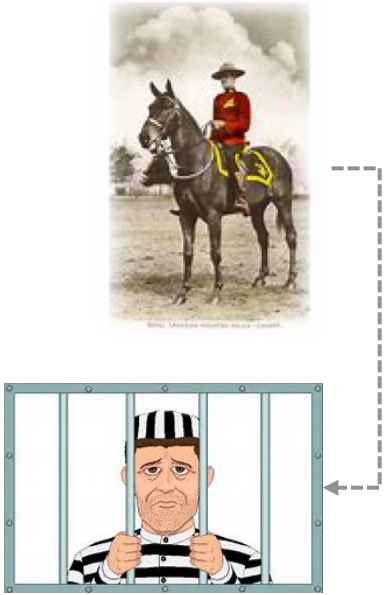
Given B need H(B) = H(B') collision
But infeasible…



…but what if:
Replace whole blockchain

Backwards compatibility

- Current products often contain older or *other* algorithms
  - Insecure: DES, RC4, RC5, MD4, MD5, and now SHA-1
  - Geopolitical algorithms (e.g. Russian GOST)
  - *Newer* algorithms (e.g. ChaCha20)
- Current products often contain older protocols
  - SSL v2.0, v3.0 and TLS v1.0, v1.1
- Choices: disuse, disable, or discard the offender
  - Vulnerability scans *always find their target*



SUMMARY

Problems: raw public keys & self-sign certificates

Implementations: OpenSSL, blockchain, backwards compatibility

Conclusions

- Cybersecurity is hot; but it's at risk
  - Poor key management undermines cryptography
  - Bad cryptography weakens cybersecurity
- Cryptography should be based on
  - Awareness of risks
  - Education
  - Experience
- Quantum Computing risks are here
  - X9 Quantum Computing Risk Study Group

CRYPT-W14
PDAC-F03

Cryptography deep dive

Appendix: References

- International Standards Organization www.iso.org
- American National Standards Institute www.ansi.org
- Accredited Standards Committee X9 www.x9.org
- National Institute of Standards and Technology www.nist.gov
  - Cryptographic Algorithm Validation Program (CAVP)
  - Cryptographic Module Validation Program (CMVP)
- National Information Assurance Partnership www.niap-ccevs.org
  - Common Criteria Evaluation and Validation Scheme (CCEVS)

Apply What You Have Learned Today

- Next week you should
  - Build awareness about how cryptography underlies your cybersecurity controls
- In the first three months following this presentation you should
  - Identify all the places where your cyber security controls rely on cryptography
  - Examine where and how the keys are managed
- Within six months you should
  - Drive a project to fix all identified gaps in secure key management
  - Upgrade old crypto implementations, if necessary