SAND2013-8088C

October 21, 2013

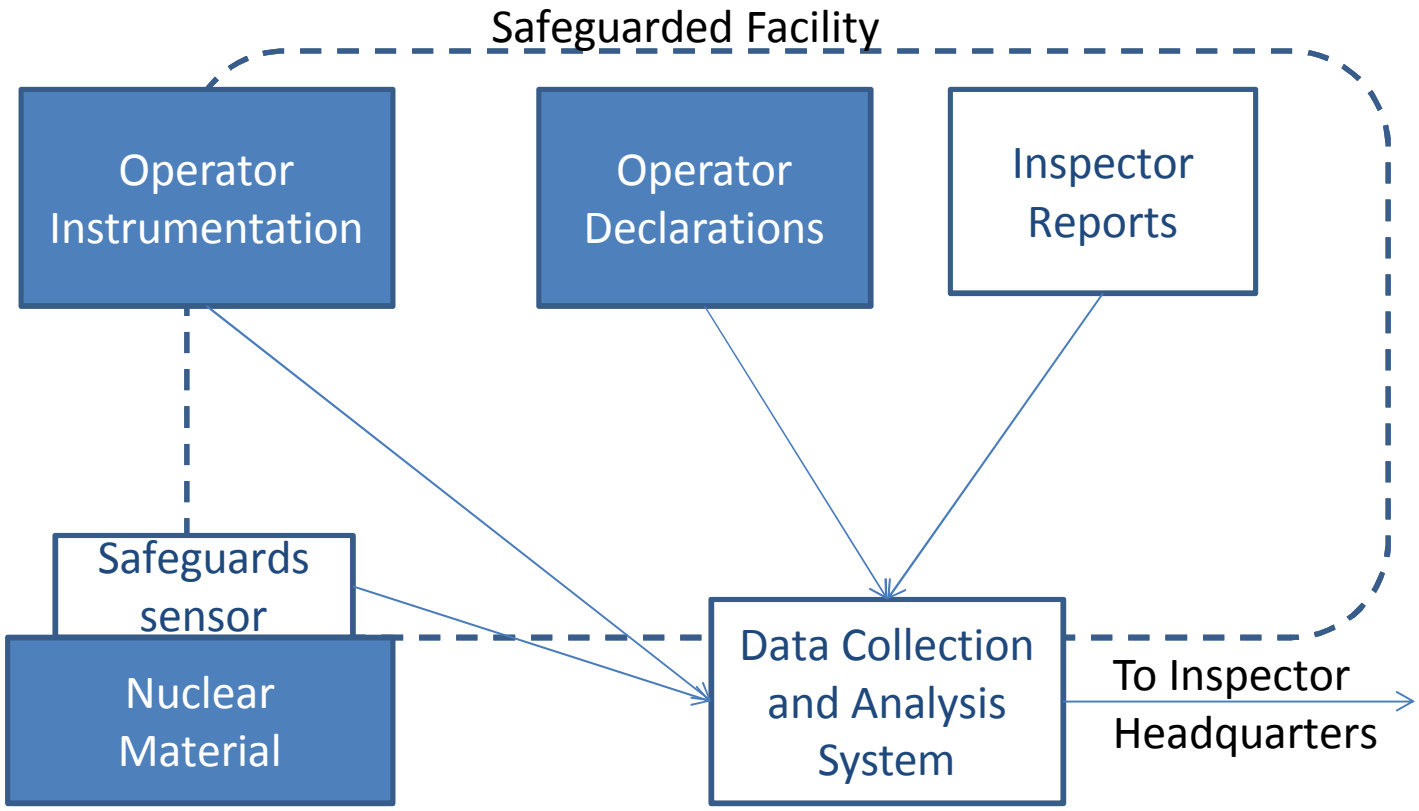
Cryptography in Safeguards NGSPN Workshop

Sandia National Laboratories

SAND 2013-XXXXC

Sandia National Laboratories is a multi program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND 2011-4678P

Facility Monitoring in Safeguards



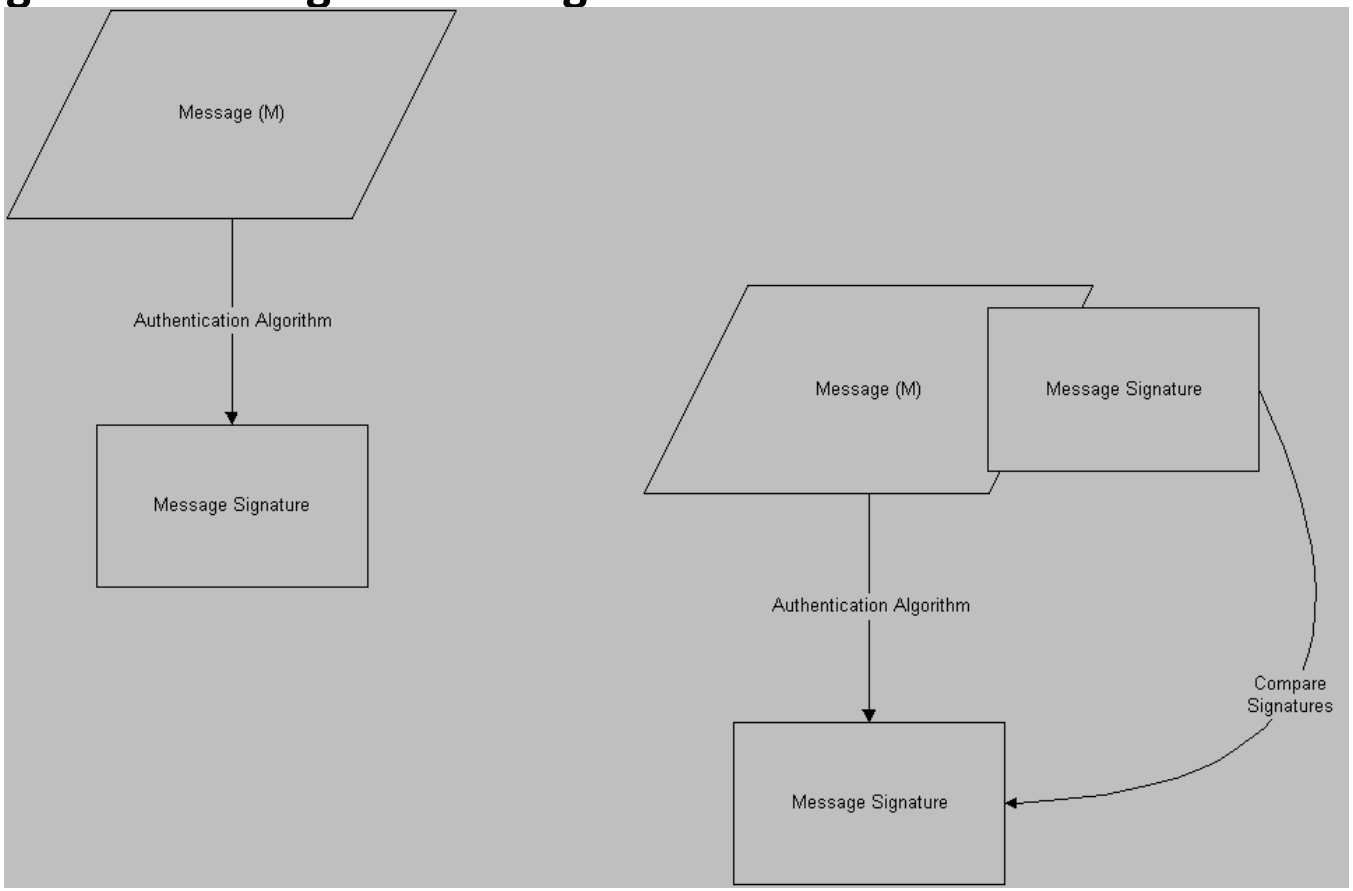
- **Problem Statement: Decreasing inspector budgets, increasing data, and highly skilled adversaries. How do you protect inspector data?**

What are the Issues?

- **We must assume that the facility operator or even a government is an adversary interested in diverting material**
  - Highly skilled
  - Unlimited resources
  - Unlimited time
- **Examples of adversary manipulation:**
  - False operator declarations
  - Disabling or tampering with inspector sensors
  - Replacing inspector sensors with tampered clone
  - Modifying, deleting, or duplicating inspector data
  - Reading inspector confidential data
- **Cryptography is a solution to some of these issues**
  - Coupled with other security features, we can decrease the likelihood of a successful attack.
  - There are multiple points of attack.

Cryptographic Authentication

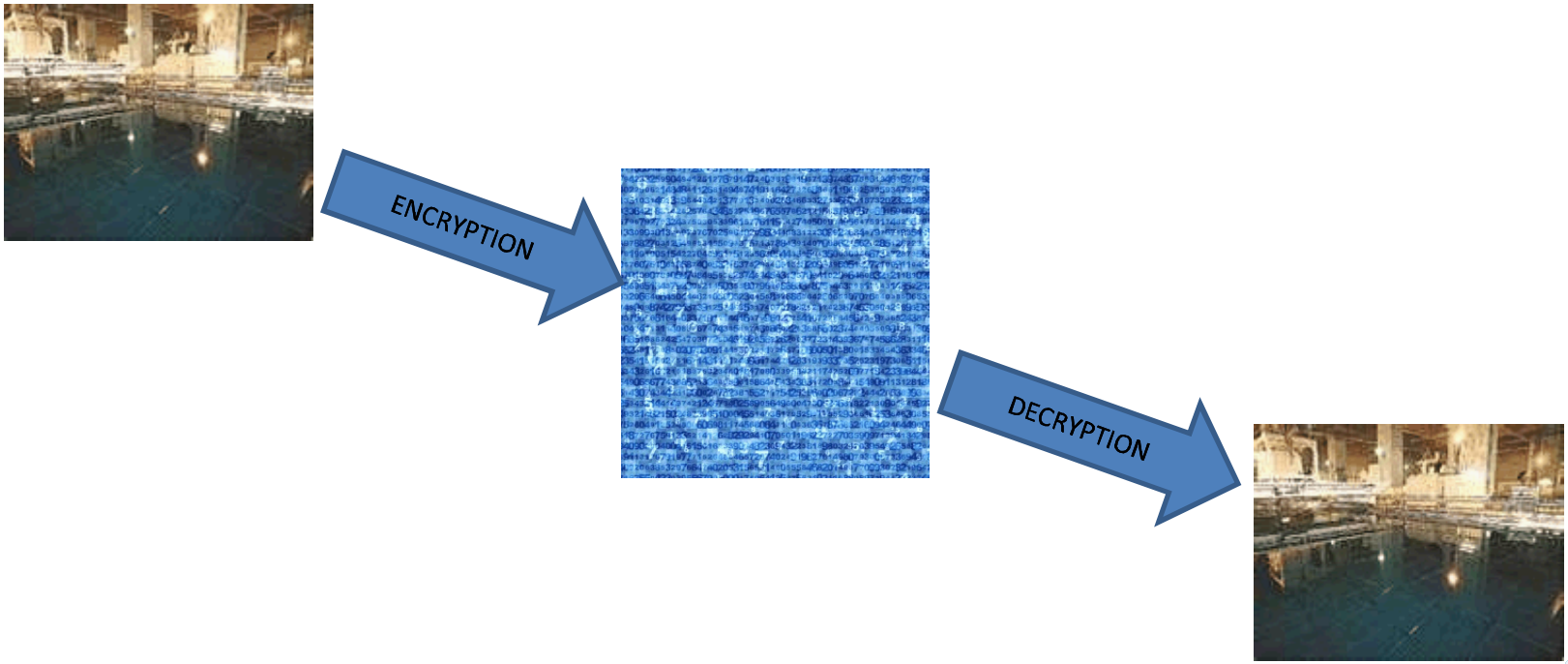
- **Prevent unauthorized deletion, insertion, or duplication of data.**
- **The data is manipulated mathematically to form a signature which is used to augment the original message**



Cryptographic Encryption

- **Data encryption is a cryptographic process that is used to alter data into an unreadable, but a reversible format**

- **This prevents unauthorized viewing of the information**

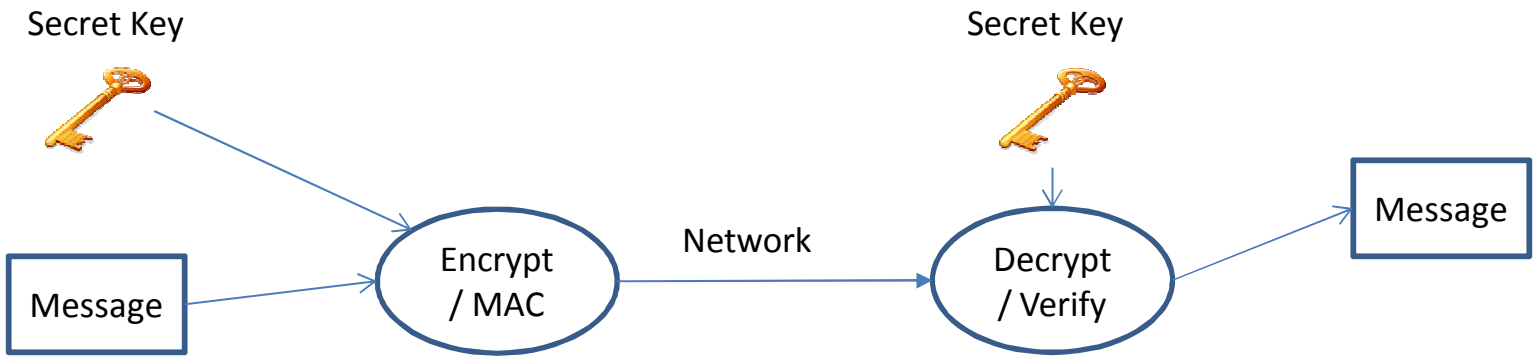


Cryptography Requires an Algorithm + Key(s)

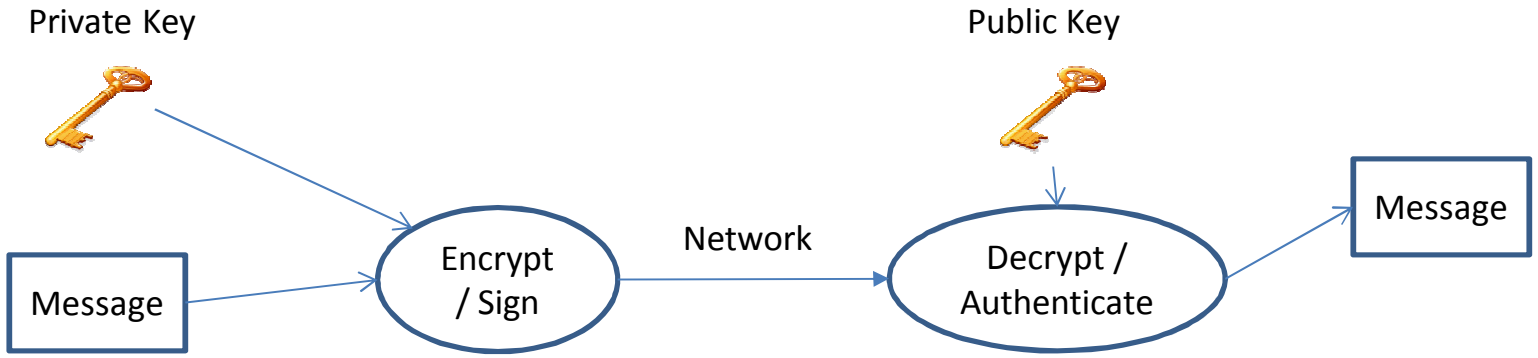
- **The algorithm performs the encryption/decryption or signing/authentication**
  - Should be openly public / not secret
  - Minimizes chance of vulnerabilities
- **A key is an additional piece of information that uniquely maps the message to the cipher text/signature**
  - Should be random
  - Should contain sufficient entropy
  - Should have sufficient strength
- **Generating a random number to make educated guessing impossible**
  - Examples: mouse movements on computer, process variations
- **Key strength to minimize chance of guessing by brute force**
  - 2^{128} combinations = 3.4×10^{38}

Cryptographic Keys

- **Symmetric Key Cryptography has a shared secret key**



- **Asymmetric Key Cryptography uses a private/public key pair**



The Key Management Issue

- **Key Management deals with the creation, storage, exchange, use, and replacement of keys.**
- **Symmetric Key Cryptography**
  - Primary cryptographic method used in safeguards historically
  - Same key resides at source and destination of data
  - A trustworthy person would have to manage those keys
  - The more shared secrets, the more complexity and vulnerability
- **Asymmetric key Cryptography**
  - Gaining traction in safeguards
  - Holder of private key can sign/encrypt
  - Holder of public key can decrypt/authenticate
  - Now possible for a sensor/system to generate a key pair and release only the public key
  - No more need for a person to manage the keys
  - How to ensure public key safely reaches destination?
- **General**
  - How to safely store keys?
  - How long do you wait before you replace keys?

Dual Use in Safeguards

- **Dual use issues can make management of cryptography even more complex**
  - E.g., IAEA and regional inspectorate, such as ABACC
  - Use of dual-controlled vessel to store keys
- **Each party could have their own sensors**
  - Extra cost
  - Extra space
- **What if each party should receive different information from dual-use equipment?**
  - Create sensors with different virtual channels which sends distinct data
  - Each channel uses distinct cryptographic key sets

Care of Cryptographic Keys

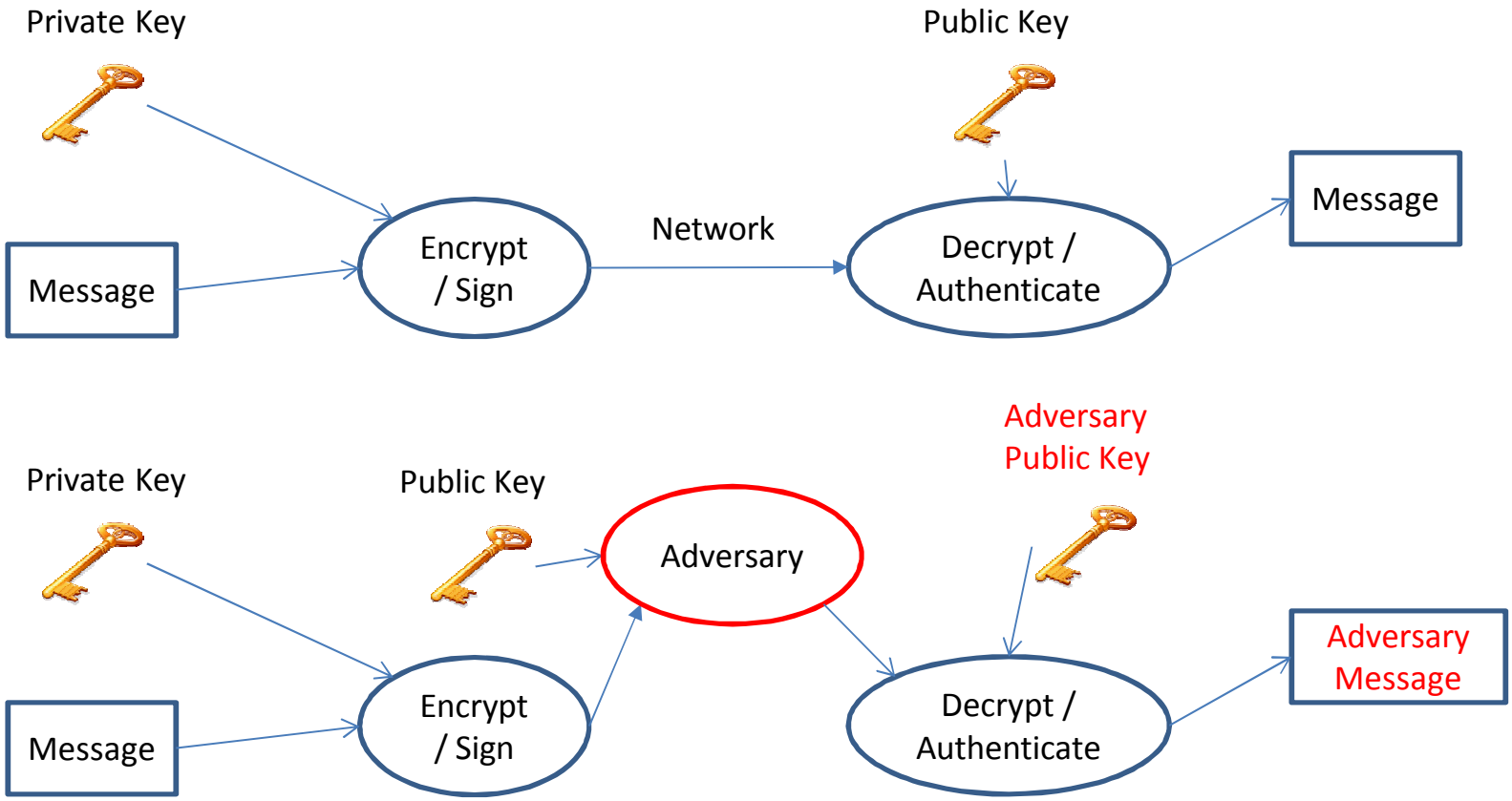
- **Must treat a cryptographic keys with care!**
  - If an adversary attains a private key, they can impersonate and/or eavesdrop
  - Poor key management
  - Tampering with a sensor
  - Insider threat
  - Keys that are not truly random
  - Poor choice of algorithm
- **Key exchange**
  - Adversary can intercept keys if exchanged electronically
  - There are key exchange algorithms that allow for more secure key exchange over insecure channels
- **Perhaps a sensor could detect a tamper attempt?**
  - In safeguards, design an enclosure that could detect tamper and erase keys
- **Many system use outdated algorithms and/or low key strength**
  - Known vulnerabilities
  - Modern computers can break cryptography quickly

Recommended Algorithms

- **The NSA recommends algorithms based on your application**
  - Suite B
  - Algorithm is open source so that community can try to break
  - Never use algorithms that are proprietary!
- **Encryption: Advanced Encryption Algorithm (AES) 128 and 256-bit**
- **Authentication: Elliptic Curve Digital Signature Algorithm (ECDSA)**
- **They also provide for key exchange and hashing (alternate way to generate authentication signature or message authentication code).**

Man in the Middle Attacks

- **When exchanging keys, what if an adversary pretended to be the sensor or inspector system?**



Certificate Authority

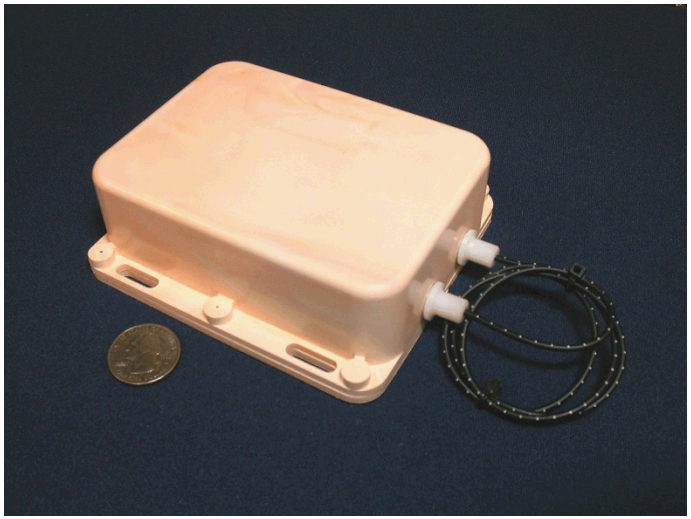
- A trusted third-party mechanism to promote trust when exchanging public keys
- The certificate authority (CA) issues certificates that certify the owner of a public key
- Concept widely used on the Internet
- In safeguards, the CA could be the inspection agency (e.g., IAEA)
- If the CA is compromised, the entire cryptographic system fails

How Hard is it to Break Cryptography?

- **This is dependent of the cryptographic algorithm, key strength, and adversary's computing power**
- **128-bit AES brute force attack (source: EE Times)**
  - There are a total of 2^{128} combinations = 3.4×10^{38}
  - Assume you have a super computer capable of 10.5×10^{15} operations/second
  - It would take 1 billion billion years to test all combinations
  - Assume you discover the correct key when you've tried 50% of the combinations
  - Very secure!
- **However, computers may continue to get exponentially faster**
  - In 20 years, who knows?
  - What about cloud computing resources?

Cryptography in SNL Safeguards

- **Surveillance**
  - SSP Camera
- **C/S Seals**
  - RMSA
- **Portal Monitoring**
- **Perimeter Monitoring**
- **Monitoring Systems**
  - Chain of Custody Backbone



- **Note that these sensors and systems communicate with hardwired and wireless connections.**

Cryptographic Considerations

- Symmetric/asymmetric key
- Algorithm
- Key length
- Key storage
- Export restrictions
- Computational performance
- Predictability of data packets
- True randomness to generate keys
- Private Key protection
- Sensor power considerations
- Insider threat
- Length of time sensor is fielded
- Overall security of system

Thank You

Questions?