SAND2012-8748C

October 2012

The NGSS, an Overview and Discussion

Sandia National Laboratories

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

.

What is the NGSS?

- At the most basic level, the NGSS is a camera-based surveillance system

- The NGSS was originally designed for use by IAEA inspectors to support verification of compliance of the Non-Proliferation Treaty (NPT)

Why camera-based surveillance?

- **In your group, take 10 minutes and identify <u>at least 5</u> reasons for using camera-based surveillance in safeguards verification?**
  - **Put each idea on its own post-it note.**

Confirm Procedures

Detect something unusual

Why camera-based surveillance?

- **What are some of the benefits of camera-based surveillance for safeguards?**

What are the potential issues with camera-based surveillance?

- **Time to THINK LIKE A BAD-GUY**

- **In your group, figure out ways a bad-guy might be able to defeat a camera-based surveillance system**
  - **E.g. Spoofing the image**
    - *Put each idea on its own post-it note.*

What are the potential issues with camera-based surveillance?

- **What are some of the potential security issues with camera-based surveillance?**

What are the potential issues with camera-based surveillance?

- **In your group, think about technical issues that could cause a camera-based surveillance system to fail**
  - **Put each idea on its own post-it note.**

What are the potential issues with camera-based surveillance?

- **What are some of the technical issues that could cause a camera-based surveillance system to fail?**

Camera-Based Surveillance

- We have identified reasons why we want to use camera-base surveillance for safeguard verification
- We, unfortunately, also identified security and technical issues associated with camera-based surveillance systems
- Now let's look at some technical solutions to protect against these security and technical issues

Someone Tampering with the System

- **Tampering includes altering the data at the electronic level or altering the physical camera (replacing it, breaking it, etc.)**

- **SOLUTIONS**
  - **Electronic tamper indicating devices**
    - *Like your own signature, each device has a unique signature which it includes with its data.*
      - This ensures the data came from the correct camera
    - *Unlike your own signature, this unique signature is also tied to the specific data*
      - This ensures the data has not been altered
  - **Physical tamper indicating devices can include:**
    - *Physical seals (EOSS)*
    - *Tamper indicating paint on enclosures*

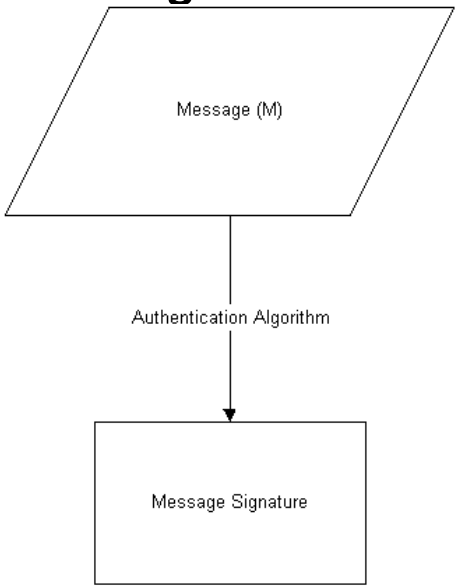
Unauthorized Viewing/Tampering with the Data

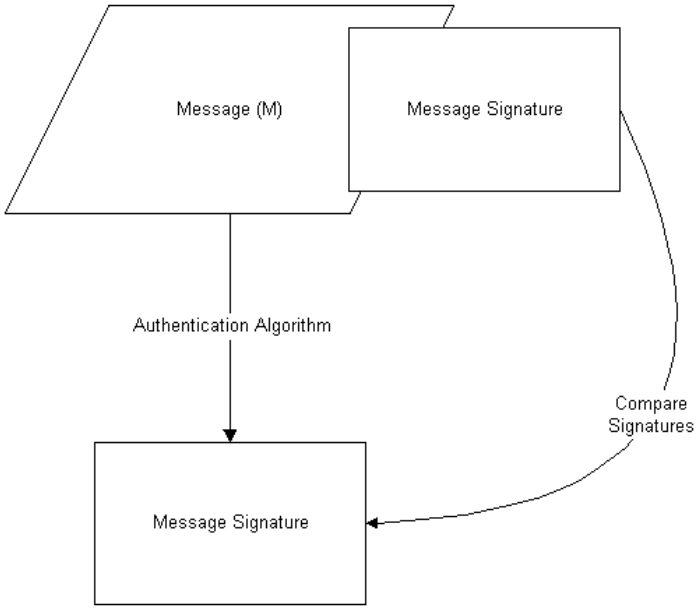
- **Someone gaining unauthorized access to the data could be through physical access to the system, pulling data off the network, hacking into the system to get the data**

- **SOLUTIONS**
  - **Cryptographic authentication at the source**
  - **Data encryption at the source**
  - **Tamper housing which destroys data (or ability to see the data)**

Cryptographic Authentication

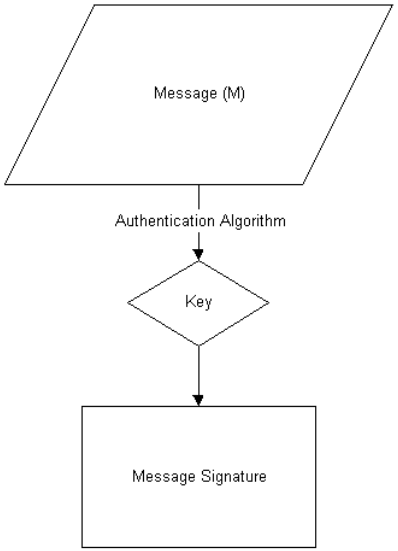
- **Prevent unauthorized deletion, insertion, or duplication of data.**
- **The data is combined mathematically to form a smaller set of data which is used to augment the original message**

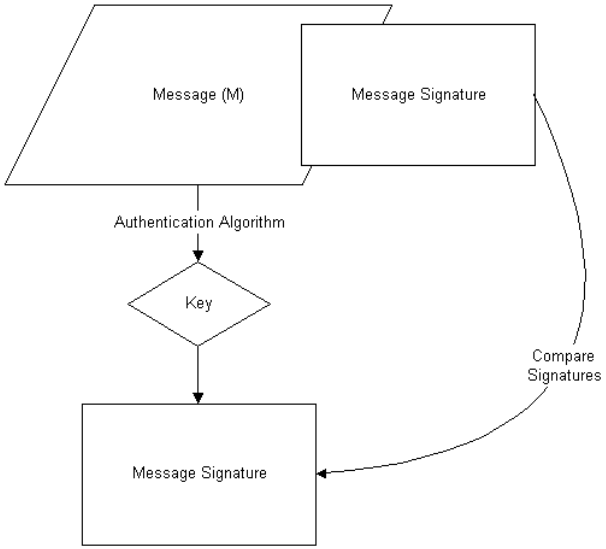




Private (Symmetric Key) Authentication

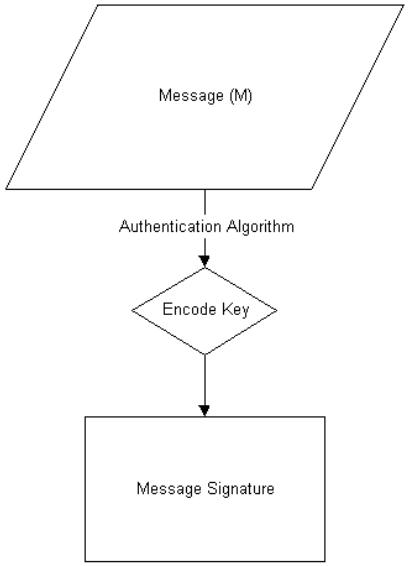
- **Uses a single key to ensure the authentic of the sender to the receiver (both have the same key)**

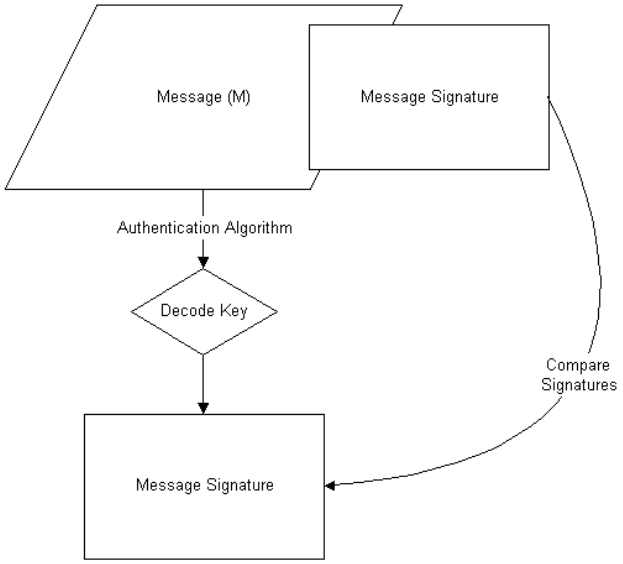




Public (Asymmetric Key) Authentication

- **Uses a single key to ensure the authenticity of the sender to the receiver (each has their own key)**

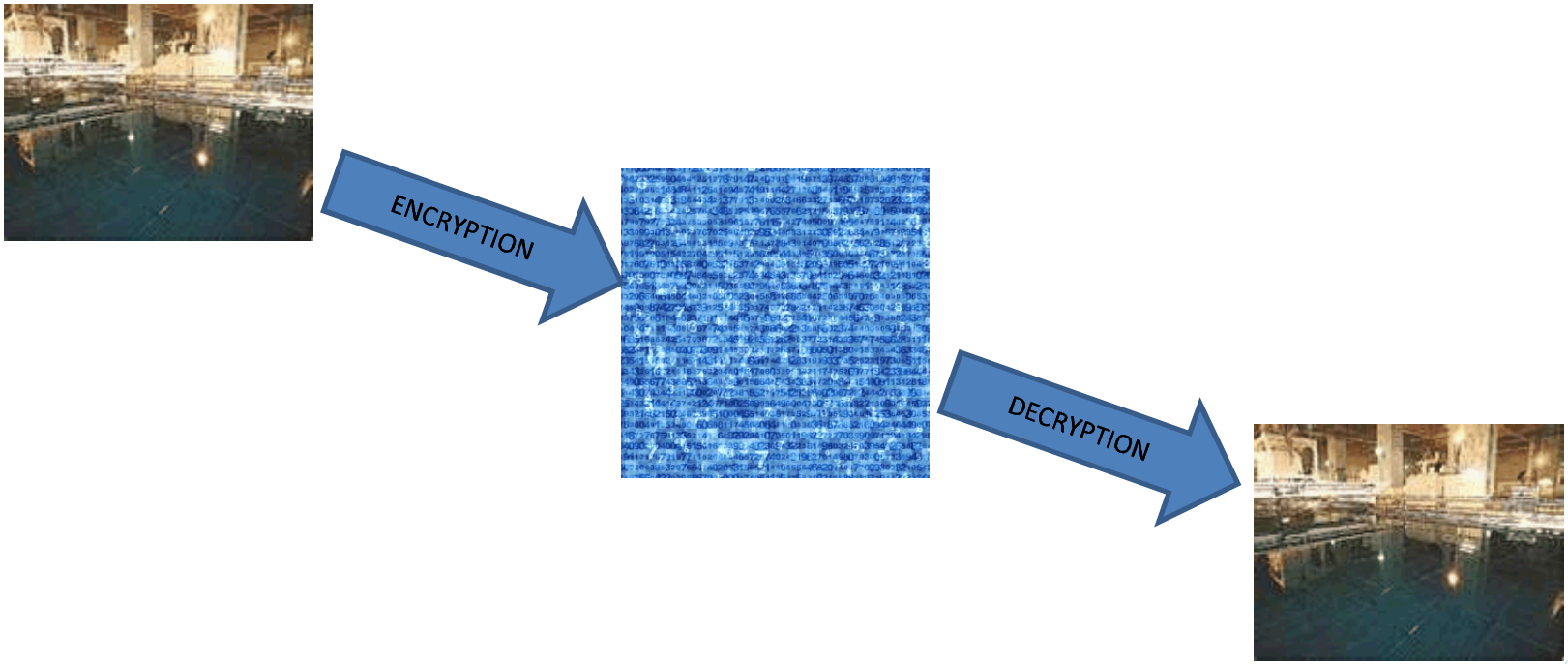




Data Encryption – a bit more detail

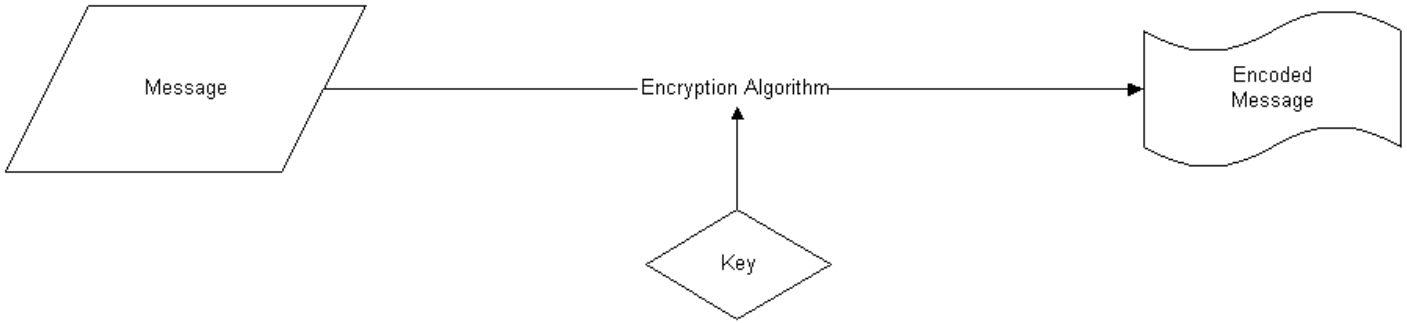
- **Data encryption is a cryptographic process that is used to alter data into an unreadable, but a reversible format**

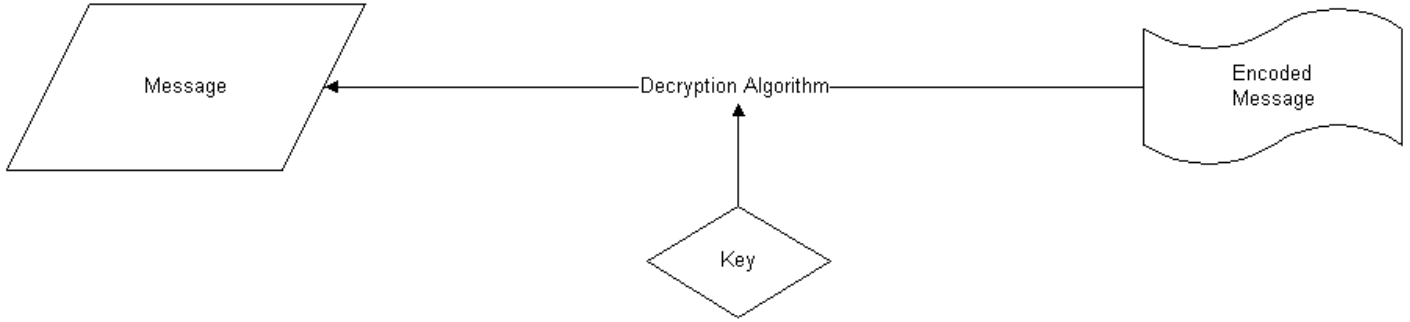
- **This prevents unauthorized viewing of the information**



Private (Symmetric Key) Encryption

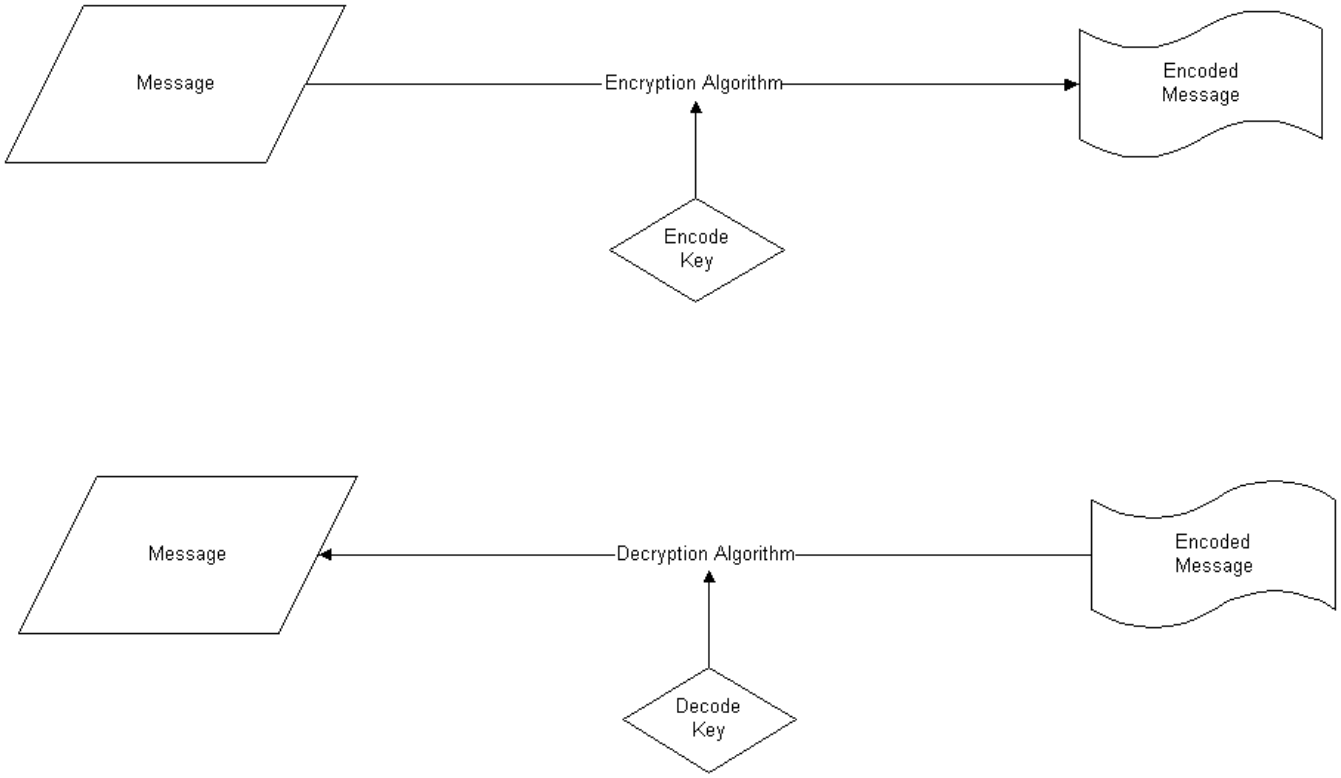
- **The same key is used to encrypt and decrypt the data**





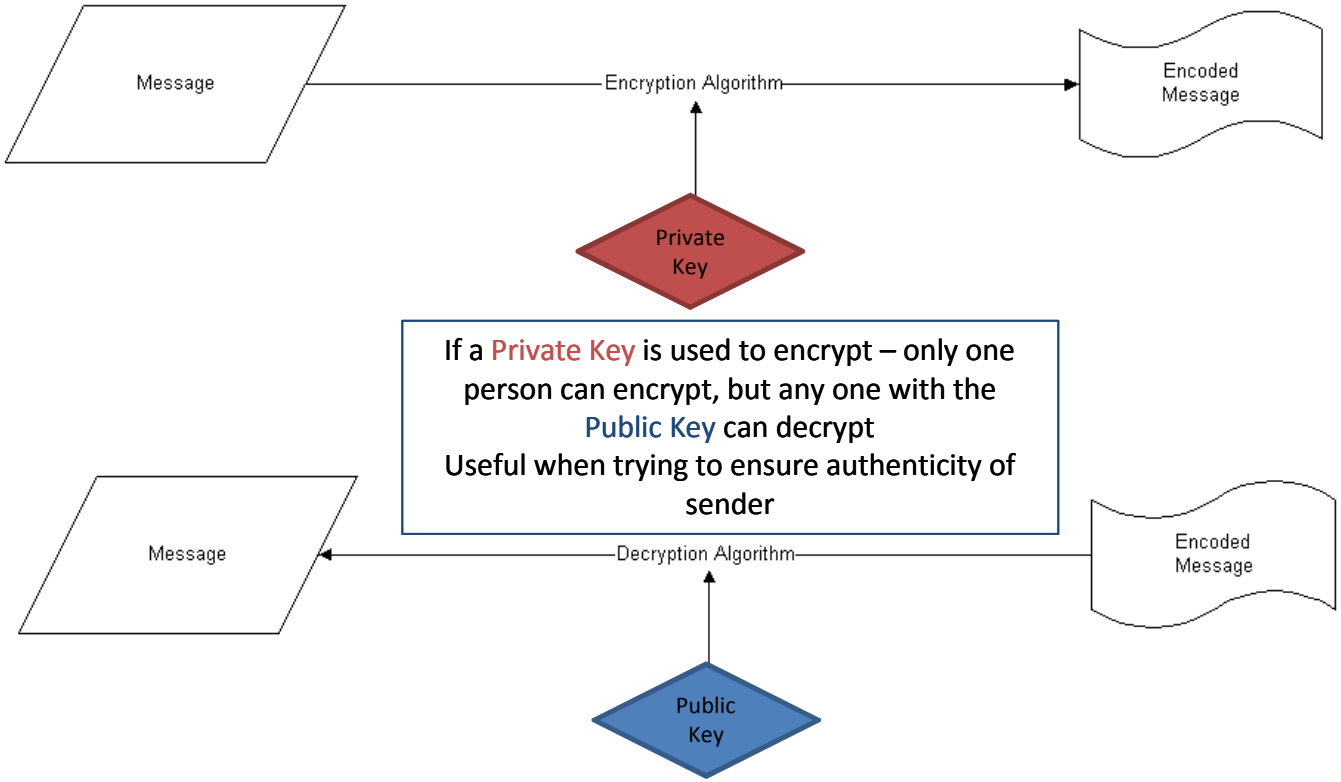
Public/Private (Asymmetric Key) Encryption

- **A separate key is used for encrypting and decrypting the data**



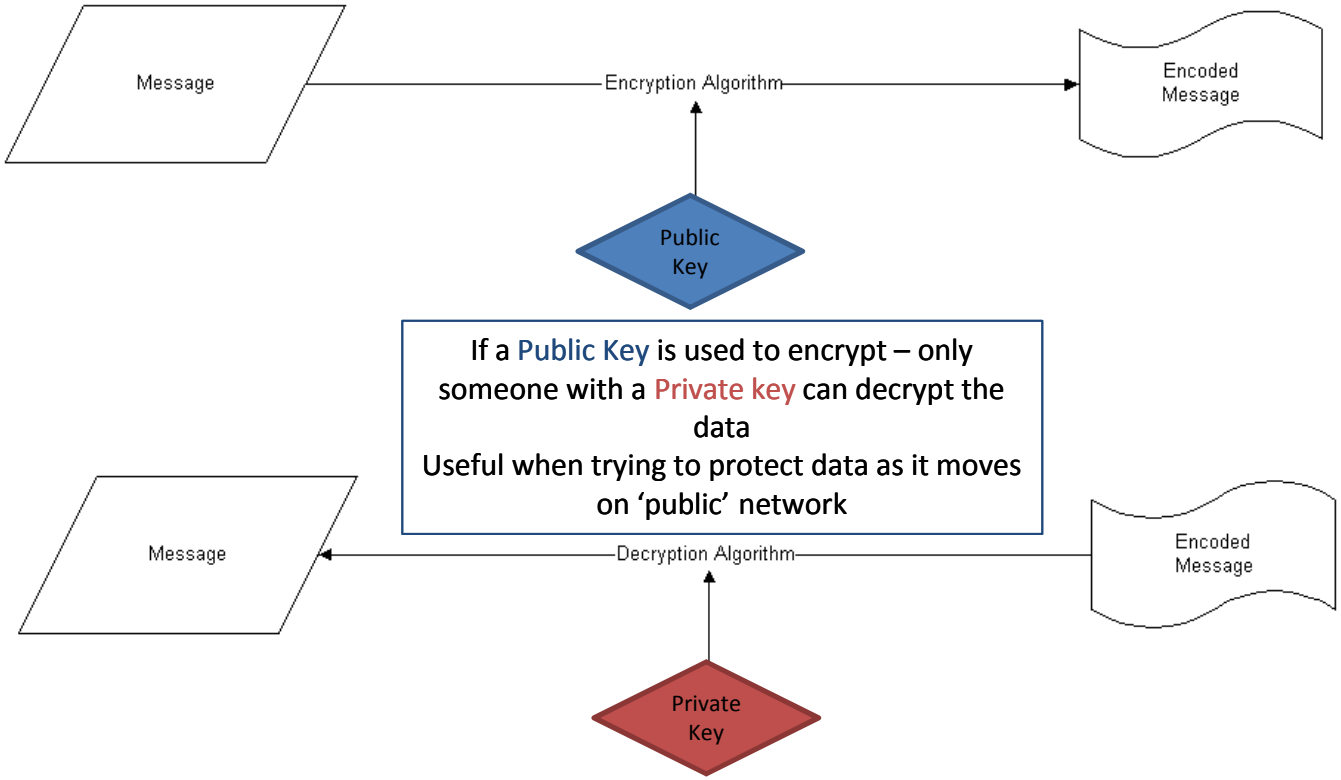
Public/Private (Asymmetric Key) Encryption

- **A separate key is used for encrypting and decrypting the data**



Public/Private (Asymmetric Key) Encryption

- **A separate key is used for encrypting and decrypting the data**



Asymmetric vs. symmetric systems

- **Asymmetric systems**
  - Slower
  - More computationally intensive
  - Easier key management
  - Need Certificate Authority (CA)
- **Symmetric systems**
  - Faster
  - Easier to implement
  - Less computational power required
  - Key management and security of keys critical to security of system

NGSS

- **Now, let's look specifically at the NGSS to see how it has been designed with measures in place to protect against security and technical issues**

Goals of NGSS

- High reliability
- “Standards-based” design
- Improved security
- Improved capabilities
- Modular components for flexibility
- Ease of maintenance and setup
- Sustainable
- Weight

NGSS Technical Features

- **Technical specifications**
  - Up to 8 Cameras per rack (DCMC5)
    - *Up to 4 virtual channels per camera*
  - Network based storage
  - IP Based communication
  - Onsite / remote configuration
- **Redundancy**
  - Redundant storage
    - *On camera*
    - *On data consolidator*
  - Redundant power
- **Security**
  - Tamper indicative housing
  - Components authenticated
  - Images encrypted

NGSS Components

- **DCMC5 Camera**
  - **Technical Specifications**
    - *5M-pixel CMOS sensor*
    - *Virtual 4 channel model*
    - *Electronic Pan/Tilt/Zoom*
    - *Up to 1 image/second*
    - *IP based communication*
    - *Status of Health messages transmitted to chassis*
  - **Redundancy**
    - *Images stored on internal SD card*
    - *Images pulled from DCMC5 and stored on multiple devices within the chassis*
    - *Battery back up on chassis*
    - *Local battery back up*
  - **Security**
    - *Images encrypted within DCMC5*
    - *Images authenticated within DCMC5*
    - *Communication to and from DCMC5 authenticated*
    - *Tamper indicative / sealable housing to destroy cryptographic keys*

Sandia National Laboratories

NGSS Components

- **Digital Camera Interface (DCI)**
  - **Technical Specifications**
    - *DCI has a one to one relationship with DCMC5*
    - *Pulls data from DCMC5*
      - Status of health
      - Images
  - **Redundancy**
    - *Stores data locally on an SD card*
    - *Shares data with the NAS*
    - *Back up power from its own UPS*
  - **Security**
    - *Housed in tamper indicative 19” rack*
  - **Backwards compatible with DCM-14**
  - **RS-485 connection to EOSS to trigger image capture**
    - *Seals may be daisy chained*

NGSS Components

- **Data Consolidator (DC) Chassis**
  - **Holds NGSS up to four NGSS sub-systems per chassis**
    - *Central Processing Unit (CPU)*
    - *Network Attached Storage (NAS)*
    - *Digital Camera Interface (DCI)*
    - *16 port Ethernet switch*
  - **Redundancy**
    - *Back up power for each sub-system*
  - **Security**
    - *Housed in tamper indicative 19” rack*

NGSS Components

- **Central Processing Unit (CPU)**
  - **Technical Specifications**
    - *Monitors all networking traffic*
    - *Handles system component discovery and configuration*
    - *Provides remote data oversight*
    - *Up to 32 cameras*
  - **Redundancy**
    - *Back up power from its own UPS*
  - **Security**
    - *Housed in tamper indicative 19” rack*

NGSS Components

- **Network Attached Storage (NAS)**
  - **Technical Specifications**
    - *Pulls data from DCI and stores locally*
    - *One to four relationship between NAS and DCMC5s*

    (One to one relationship if DCMC5 in 4 channel mode)
  - **Redundancy**
    - *Mirrored 128 G-byte solid state drives*
    - *Field replaceable*
    - *Back up power from its own UPS*
  - **Security**
    - *Housed in tamper indicative 19” rack*

DCM-C5 Security

- **Master key encrypts all private keys stored on camera**
- **Camera images are authenticated then encrypted for storage on SD card**
  - **DSA2K authentication**
  - **AES 128-bit CBC-mode encryption**
- **Communications**
  - **Transport Layer Security (TLS) used for encrypted and authenticated communications**
  - **Several cipher suites supported**
- **Certificates**
  - **Inspectorate acts as certificate authority (CA)**
  - **The camera must store up to seven certificates, depending on selected cipher suite**
    - *DSA signing: certificate for authentication of images and possibly communication, which must be signed by CA. Camera is owner of private key.*
    - *RSA signing: optionally used for communications, the camera can generate a certificate request to be signed by the CA. Camera is owner of private key.*
    - *Trusted Certificate Authority: optionally used for TLS communication with clients.*
    - *Encryption Channel 1-4: Up to four RSA certificates for encryption of each channel*
- **Access levels**
  - **Root: Client can command and query camera, requires a certificate and password**
  - **User: Client receives all camera data, query information, and requires a certificate**
  - **Device: A client receives encrypted information only**

NGSS Web Interface System Configuration

- The NGSS system includes an optional touch-panel display attached to the CPU subsystem for touch-screen access to the NGSS Web Interface for system configuration.

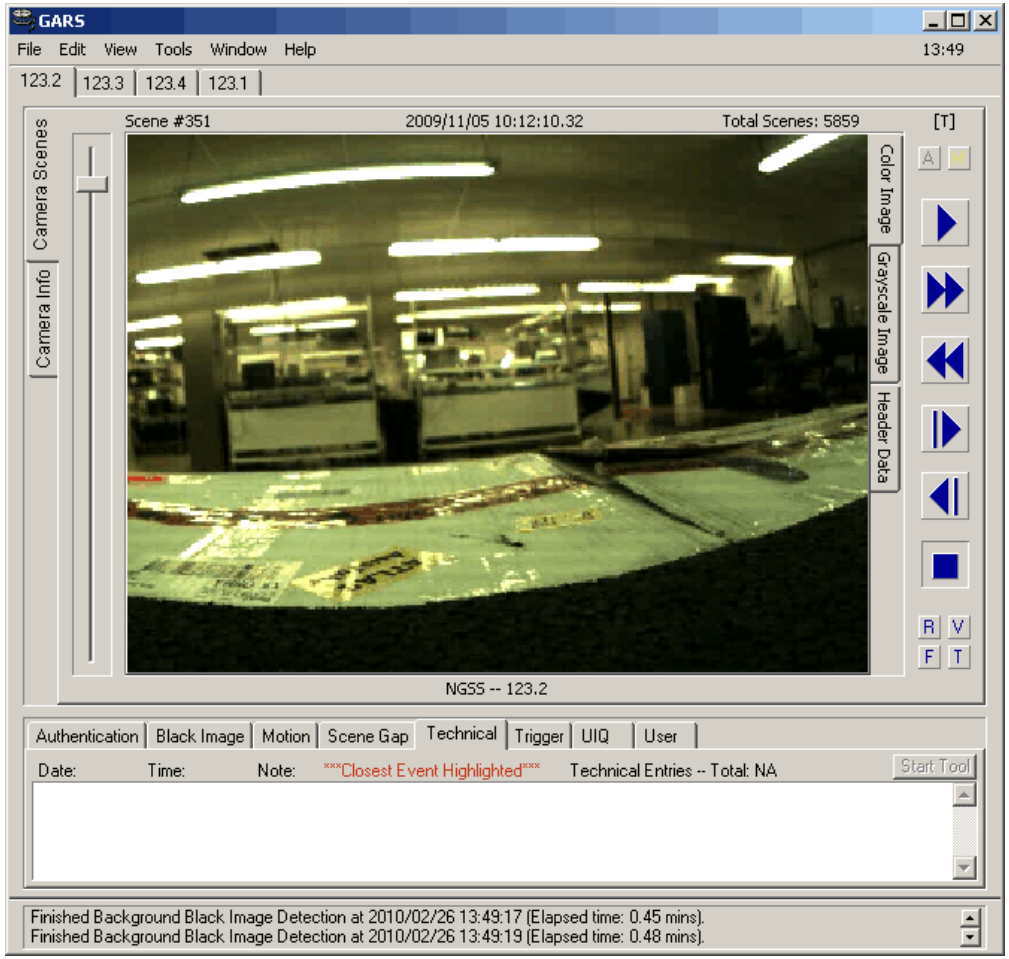
Cryptotoken (with valid certificates) + password required for system access

Sandia National Laboratories

NGSS Review Software

- **Software is a modified version of GARS**

- **Decryption**
- **Authentication**
- **State of Health**
- **Image Processing**



Sandia National Laboratories

The NGSS

- **The NGSS is a camera-based surveillance system with specific measures implemented to ensure technical reliability and security**

Crypto Details

Transport Layer Security (TLS) Cipher Suites

- **DHEDSS-AES128CBC-SHA256 (0x0040), DHEDSS-AES128CBC-SHA1 (0x0032), DHERSA-AES128CBC-SHA256 (0x0067), DHERSA-AES128CBC-SHA1 (0x0033), RSA-AES128CBC-SHA256 (0x003C), RSA-AES128CBC-SHA1 (0x002F).**

- **Key exchange**
  - Diffie-Hellman using DSS certificate
  - Diffie-Hellman using RSA certificate
  - RSA
- **Encryption**
  - AES 128-bit CBC
- **Authentication**
  - SHA1
  - SHA256