Grid Security

Grid security is a crucial component

- Need for secure communication between grid elements
  - Authenticated (verify entities are who they claim to be -> use certificates and CAs)
  - Confidential - only invited to understand conversation (use encryption)
- Need to support security across organizational boundaries
  - No centrally managed security system
- Need to support "single sign-on" for users of grid
  - Delegation of credentials for computations that involve multiple resources and/or sites
  - allowing or denying access to services based on policies (authorization)

Identity & Authentication

- Each entity should have an identity
- Authenticate: Establish identity
  - Is the entity who he claims he is ?
  - Examples:
    - Driving License
    - Username/password
- Stops masquerading imposters
  - A secure communication should ensure that the parties involved in the communication are who they claim to be.

Authorization

- Establishing rights
- What can a certain identity do ?

Examples:

- Are you allowed to be on this flight ?
  - Passenger ?
  - Pilot ?
- Unix read/write/execute permissions

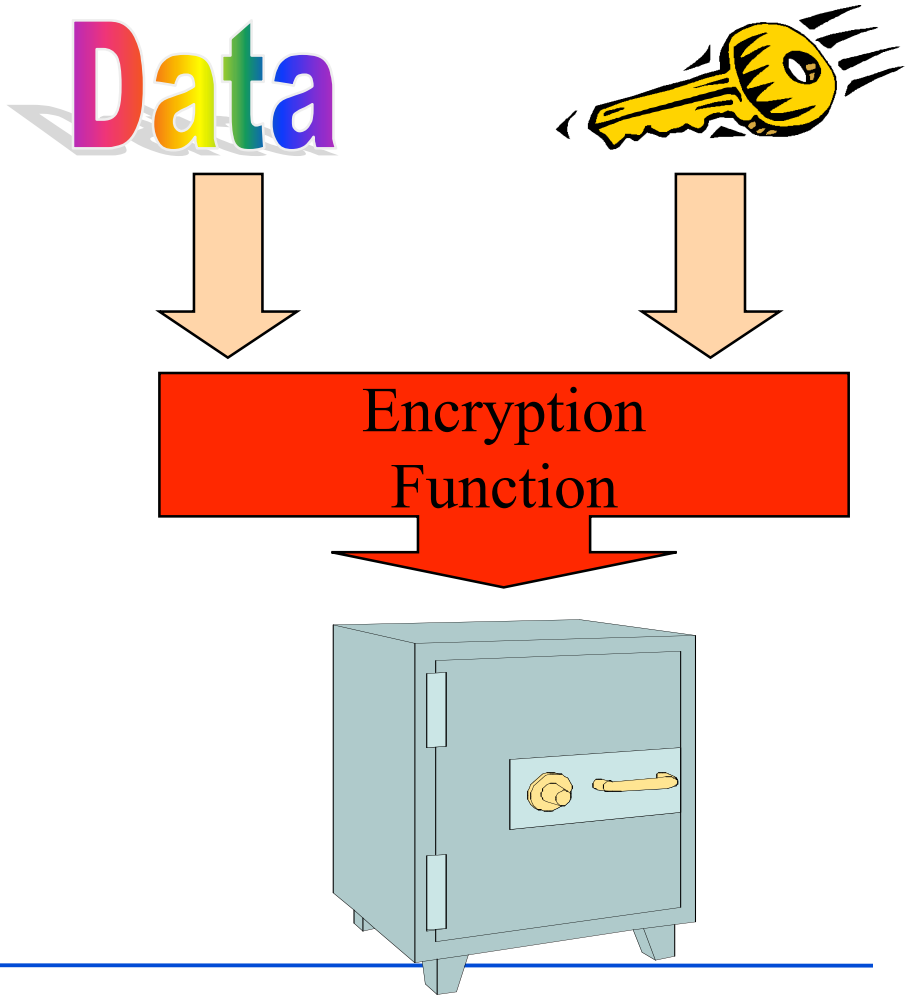
- *Must authenticate first*

Single Sign-on

- Important for complex applications that need to use Grid resources
  - Enables automation of processing
  - Allows remote processes and resources to act on user's behalf --> Delegation
  - Enables easy coordination of varied resources

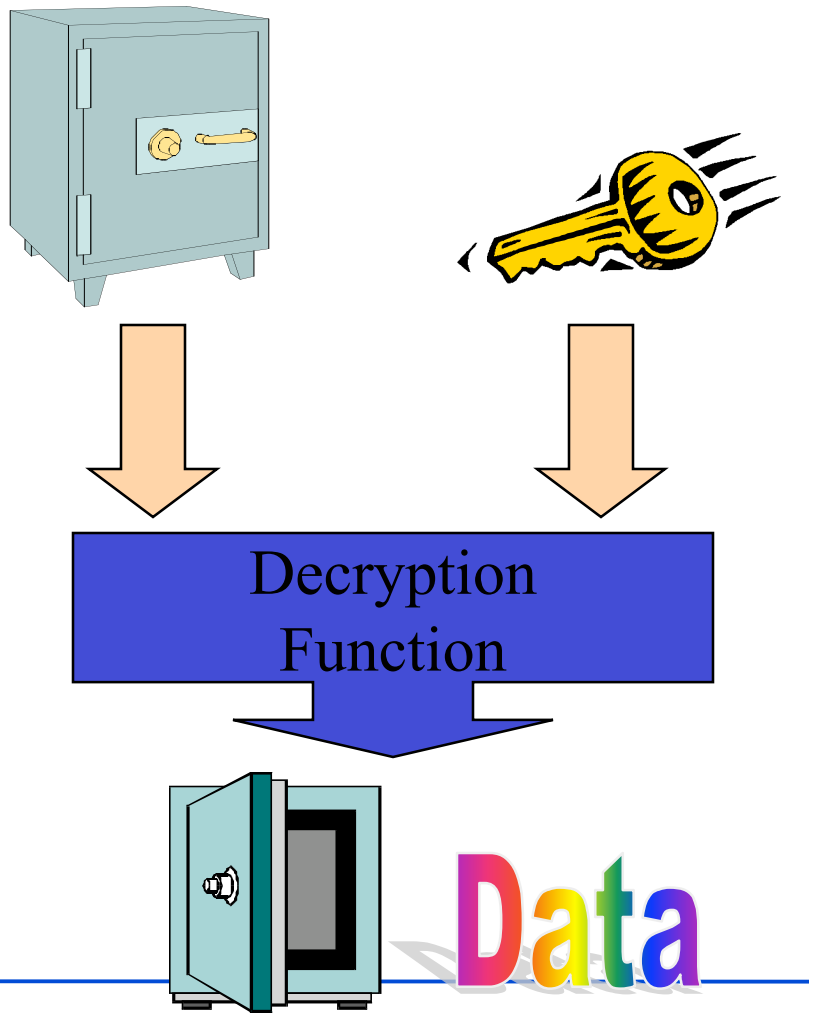
Encryption

- Encryption is the process of taking some data and a key and feeding it into a function and getting encrypted data out
- Encrypted data is, in principal, unreadable unless decrypted



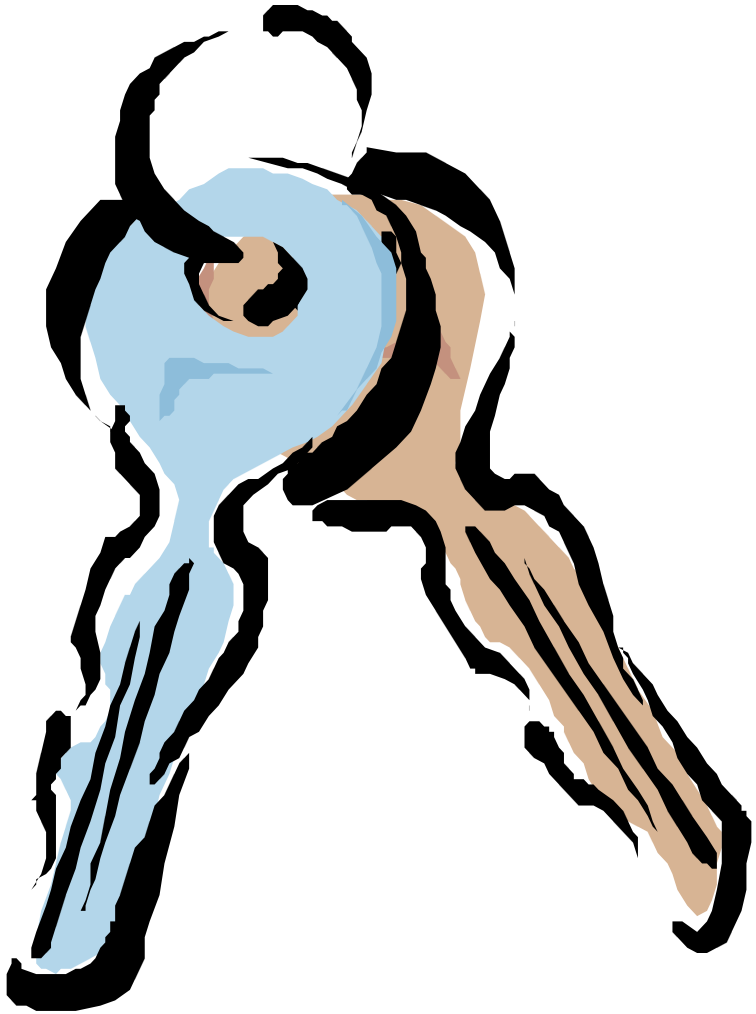
Decryption

- Decryption is the process of taking encrypted data and a key and feeding it into a function and getting out the original data
  - Encryption and decryption functions are linked



Asymmetric Encryption

- Encryption and decryption functions that use a key pair are called asymmetric
  - Keys are mathematically linked



Public and Private Keys

- With asymmetric encryption each user will be assigned a key pair:

  a **private key** and a **public key**

Private key is known only to owner

Public key is given away to the world

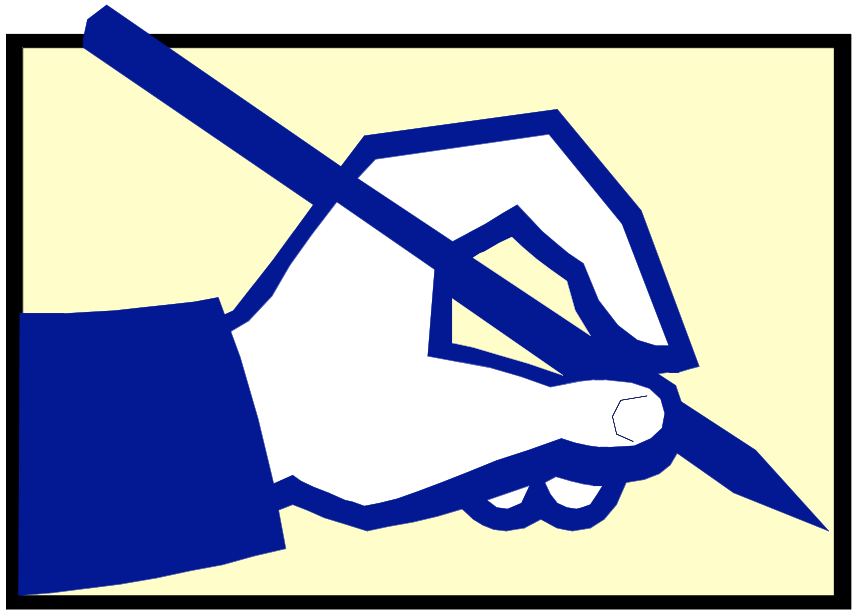
- Encrypt with public key, can decrypt with only private key
- Message Privacy -> integrity of the message is guaranteed

Public Key Infrastructure (PKI)

- PKI allows you to know that a given public key belongs to a given user
- PKI builds off of asymmetric encryption:
  - Each entity has two keys: public and private
  - The private key is known only to the entity
- GSI is based on PKI
- The public key is given to the world encapsulated in a X.509 certificate

Digital Signatures

- Digital signatures allow the world to
  - determine if the data has been tampered
  - verify who created a chunk of data
- Sign with private key, verify with public key
- Message Integrity



Certificates

- Central concept in GSI authentication
  - A public key certificate (or identity certificate) is an electronic document which incorporates a digital signature to bind together a public key with an identity
  - The certificate can be used to verify that a public key belongs to an individual
- Every user, resource and service on Grid is identified via a certificate
- Contains:
  - **Subject name (identifies entity)**
  - **Corresponding public key**
  - **Identity of the CA that has signed the cert (***to certify that the public key and the identity both belong to the subject***)**
  - **The digital signature of the CA**

Certificates

- the public key is embedded in the digital certificate, which needs to be signed by this trusted CA.
  - This way, any one who trusts the CA, can verify the validity of the public key, meaning that it confirms that this public key belongs to the rightful owner.

- GSI certs are encoded in a X509 certificate format

Certification Authorities (CAs)

- A Certification Authority is an entity that exists to sign user certificates
- A CA issues digital certificates which contain a public key and the identity of the owner.
  - CA attests that the public key contained in the certificate belongs to the person/organization/server/entity noted in the certificate.
  - CA's obligation in such schemes is to **verify** applicant's credentials, so that users and relying parties can trust the information in the CA's certificates.
- if

  (user trusts the CA) && (user can verify the CA's signature)

  then

  user can also verify that a certain public key does indeed belong to whoever is identified in the certificate

Many CA's exist

- Indeed, many CA providers exist
- ESNet:
  - **DOEGrids (doegrids.org)**

ESnet operates the DOE Grids Certificate Services to support Scientists and Engineers working on DOE related scientific efforts. This service is designed to support the new Computational Grids being deployed around the world. The service issues Identity Certificates to individual subscribers and Service certificates for Grid Services. The business model in Grids is the formation of Virtual Organizations (VO) focused on a particular scientific topic. They are currently supporting a number of VOs engaged in DOE research (among which OSG, and in particular the OSGEDU VO, to which you belong). This VO (and others) require the use of certificates that are trusted in the global research community. ESnet is actively working with the Global Grid Forum, the European Data Grid and Cross Grid CA managers to insure that DOE Grids Certificates have the widest possible acceptance.

  - ESNet Root
  - NorduGrid
  - Russian Data Intensive Grid

Globus Security:

- GSI - is a set of tools, libraries and protocols used in Globus to allow **users** and **applications** to securely access resources.
- Based on PKI
- Uses Secure Socket Layer for authentication and message protection
  - Encryption
  - Signature
- Adds features needed for Single-Sign On
  - Proxy Credentials
  - Delegation

Authorization - Gridmap

- **Gridmap** is a list of mappings

  allowed DNs --> user name

  "/C=US/O=Globus/O=ANL/OU=MCS/CN=Ben Clifford" benc
  "/C=US/O=Globus/O=ANL/OU=MCS/CN=MikeWilde" wilde
  (in /etc/grid-security/grid-mapfile directory)

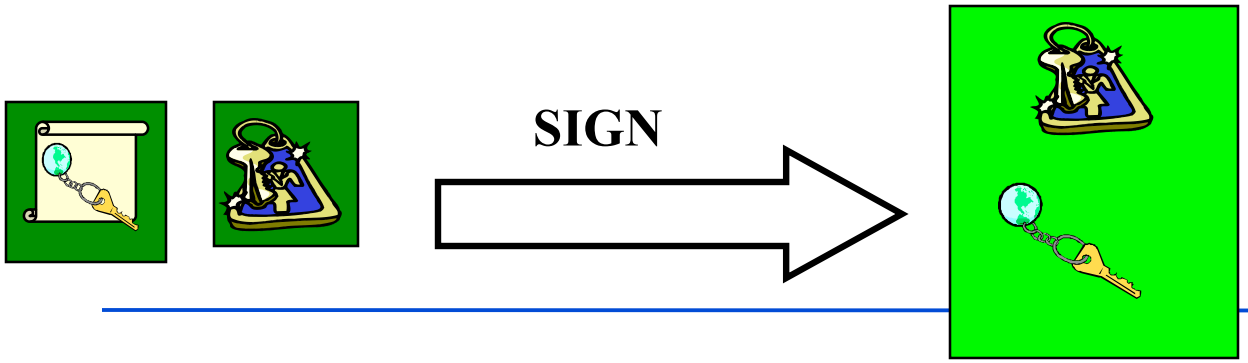
- Controlled by administrator
- Open read access

GSI: Credentials

- In the GSI system each user has a set of credentials they use to prove their identity on the grid
  - Consists of a X509 certificate and private key
- **Long-term** private key is kept encrypted with a pass phrase
  - Good for security, inconvenient for repeated usage
  - Do not lose this phrase !

GSI: Proxy Credentials

- Proxy credentials are ***short-lived*** credentials created by user
  - Proxy is signed by owner, rather than the CA
  - Short term binding of user's identity to alternate private key
  - Same effective identity as certificate



GSI: Proxy Credentials

- A proxy credential contains
  - The proxy certificate (signed by the user, and not CA)
  - Corresponding private key
    - can be kept unencrypted for easy repeated access
    - Therefore, once a proxy is created and stored, user cn use proxy certificate and private key for mutual authentication without entering a password
- Chain of trust
  - Trust CA -> Trust User Certificate -> Trust Proxy

Authorization components

- GUMS
- VOMS
- VOMRS

GUMS = Grid User Management System

- is a Grid Identity Mapping Service
- It maps the credential for each incoming job at a site to an appropriate site credential, and communicates the mapping to the gatekeeper.
- GUMS is particularly well suited to a heterogeneous environment with multiple gatekeepers;
- it allows the implemenation of a single site-wide usage policy, thereby providing better control and security for access to the site's grid resources. Read more at http://grid.racf.bnl.gov/GUMS/.

VOMS = Virtual Organization Membership Sevice

- is a system that manages real-time user authorization information for a VO
- designed to maintain only general information regarding the **relationship of the user with his VO**, e.g., groups he belongs to, certificate-related information, and capabilities he should present to resource providers for special processing needs.
- it maintains no personal identifying information besides the certificate.

When a user submits a job, assuming the user is in good standing, VOMS also creates the necessary short-term credentials (extended proxy), required by grid resources before allowing the job to run.

VOMRS = VO Management Registration Service

- major component of the extension to VOMS.
- VOMRS is a server that provides the means for registering members of a VO, and coordination of this process among the various VO and grid resource administrators
- maintains additional information on each VO member as required by individual grid resource providers, and some institution- and site-specific information.
- VOMRS relies on the VOMS system to generate extended proxies for users as needed

Grid Security - in practice - steps:

- Get certificate from relevant CA
  - DOEGrids in our case
- Request to be authorized for resources
  - Meaning you will be added to the OSGEDU VOMS (for example)
- Generate proxy as needed
  - Using grid-proxy-init
- Run clients
  - Authenticate
  - Authorize
  - Delegate as required

Numerous resources, different CAs, numerous credentials