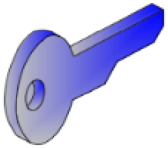
سبر1213
Network Defense

Lecture #10 Part 1

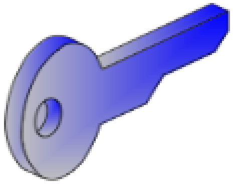
Understanding Cryptography and PKI

Providing Confidentiality with Encryption

- Two basic components of encryption
  - Algorithm
    - Performs mathematical calculations on data
    - Algorithm always the same
  - Key
    - A number that provides variability
    - Either kept private and/or changed frequently

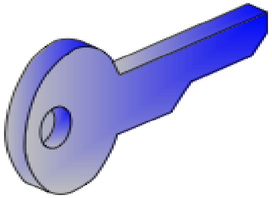


Symmetric Encryption



- Uses the same key to encrypt and decrypt data
  - When transmitting encrypted data
    - Uses key to encrypt data before transmission
    - Uses same key to decrypt data when received
- Much more efficient encrypting large amounts of data than asymmetric encryption
- RADIUS uses symmetric encryption

Simple Symmetric Encryption Example



- Encryption algorithm uses substitution cipher
  - Move forward ____ spaces to encrypt
  - For example, move forward 3 spaces to encrypt
- Decryption algorithm
  - Move back ____ spaces to decrypt
  - For example, move back 3 spaces to decrypt
- With the key of 3
  - Message is PASS and encrypted it is SDVV
- ROT13 always uses a key of 13

Block vs. Stream Ciphers

- Block ciphers
  - Encrypts data in specific sized blocks
    - Often 64-bit blocks or 128-bit blocks
  - Divides large files or messages into these blocks
  - Encrypts each block separately
- Stream ciphers
  - Encrypt data as a single bit or byte at a time in a stream
  - An important principle when using a stream cipher
    - Encryption keys should never be reused
    - If a key is reused, it is easier to crack the encryption

Symmetric Algorithms

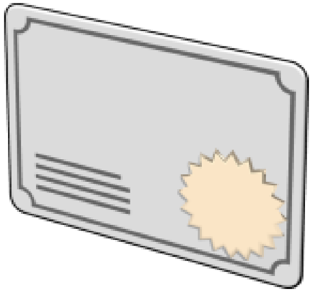
- Advanced Encryption Standard (AES)
  - Fast, efficient, strong symmetric block cipher
  - 128-bit block cipher
  - Uses 128-bit, 192-bit, or 256-bit keys

- Blowfish and Twofish
  - Strong symmetric block cipher (widely used)
  - 64-bit blocks
  - Supports between 32 and 448 bits

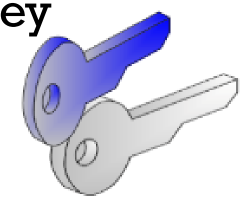
Symmetric Algorithms

- 3DES
  - 64-bit block cipher
  - Originally designed as a replacement for DES
  - Uses multiple keys and multiple passes
  - Not as efficient as AES
  - 3DES is still used in some applications, such as when hardware doesn't support AES

Asymmetric Encryption

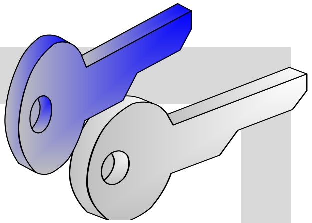


- Private Key / Public Key matched pair
  - One key encrypts, the other key decrypts
  - Only a private key can decrypt information encrypted with a matching public key
  - Only a public key can decrypt information encrypted with a matching private key
  - Private key stays private
  - Public key shared in a certificate
  - Asymmetric encryption methods require certificate and PKI

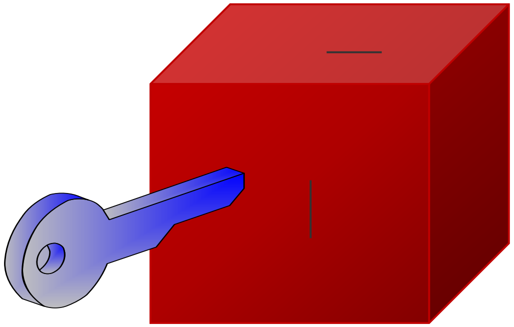


- Key exchange
  - Used to share cryptographic keys between two
    entities
  - Asymmetric encryption uses key exchange to share a symmetric key

Asymmetric Encryption

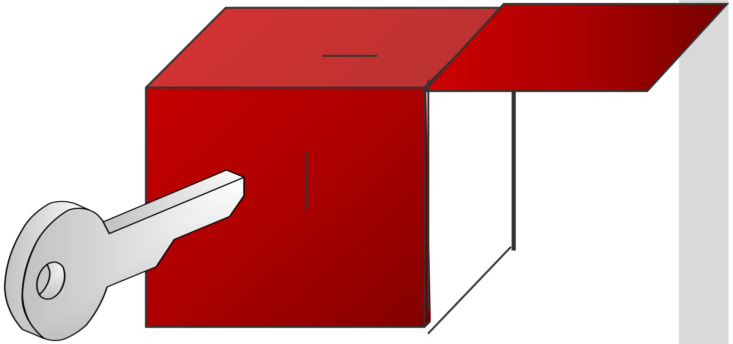


- Rayburn Box



Rayburn Box

Locked by one key



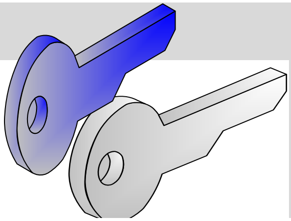
Rayburn Box

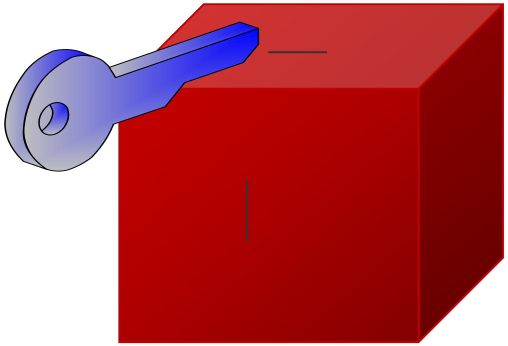
Unlocked by the other key

Asymmetric Encryption

Asymmetric Encryption

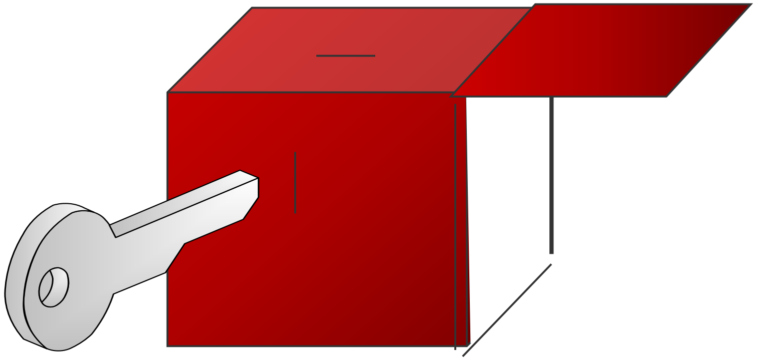
- Rayburn box used to send secrets
  - Encryption





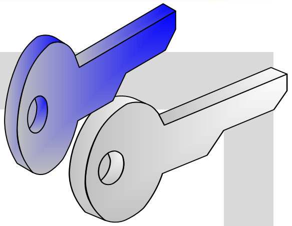
Rayburn Box

Locked by one key

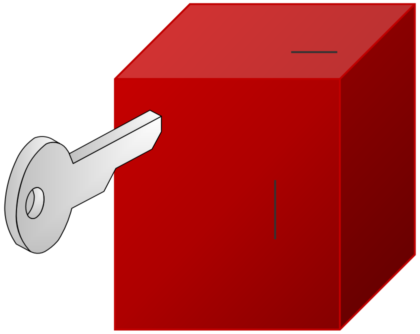


Rayburn Box

Unlocked by the other key

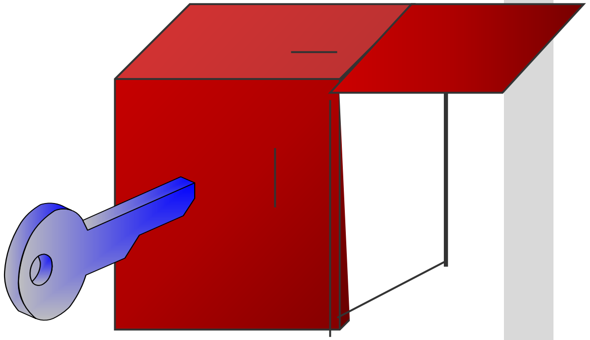


- Rayburn box used for authentication
  - Digital signature



Rayburn Box

Locked by one key



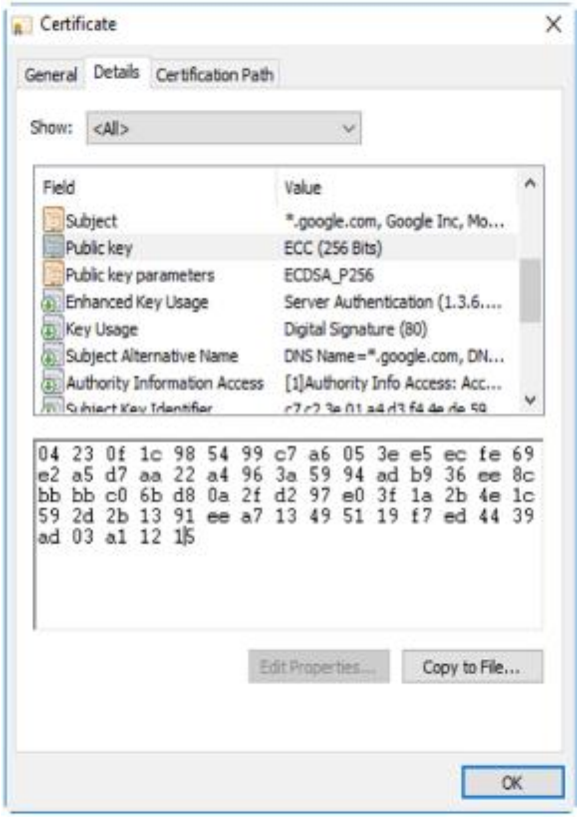
Rayburn Box

Unlocked by the other key

Asymmetric Encryption

Certificates

- Used for
  - Encryption
  - Authentication
  - Digital signatures



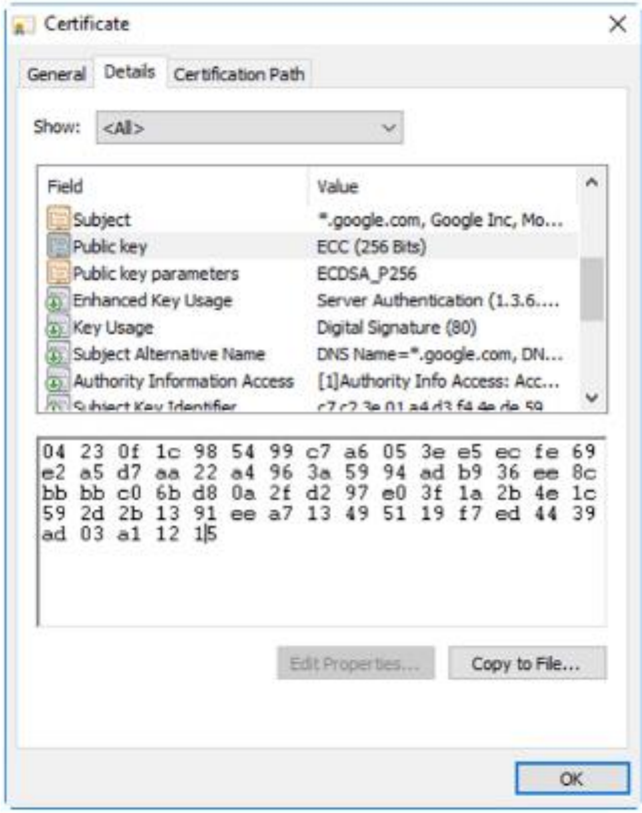
Show: <All>

Field	Value
Subject	*.google.com, Google Inc, Mo...
Public key	ECC (256 Bits)
Public key parameters	ECDSA_P256
Enhanced Key Usage	Server Authentication (1.3.6....
Key Usage	Digital Signature (80)
Subject Alternative Name	DNS Name=*.google.com, DN...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Key Identifier	c7 c2 3e 01 a4 d3 f4 4e de 59

```
04 23 0f 1c 98 54 99 c7 a6 05 3e e5 ec fe 69
e2 a5 d7 aa 22 a4 96 3a 59 94 ad b9 36 ee 8c
bb bb c0 6b d8 0a 2f d2 97 e0 3f 1a 2b 4e 1c
59 2d 2b 13 91 ee a7 13 49 51 19 f7 ed 44 39
ad 03 a1 12 15
```

Certificates

- Includes
  - Serial number
  - Issuer
  - Validity dates
  - Subject
  - Public key
  - Usage



Show: <All>

Field	Value
Subject	*.google.com, Google Inc, Mo...
Public key	ECC (256 Bits)
Public key parameters	ECDSA_P256
Enhanced Key Usage	Server Authentication (1.3.6....
Key Usage	Digital Signature (80)
Subject Alternative Name	DNS Name=*.google.com, DN...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Key Identifier	c7 c2 3e 01 a4 d3 f4 4e de 59

```
04 23 0f 1c 98 54 99 c7 a6 05 3e e5 ec fe 69
e2 a5 d7 aa 22 a4 96 3a 59 94 ad b9 36 ee 8c
bb bb c0 6b d8 0a 2f d2 97 e0 3f 1a 2b 4e 1c
59 2d 2b 13 91 ee a7 13 49 51 19 f7 ed 44 39
ad 03 a1 12 15
```