# Advanced Asymmetric Cryptography Concepts

Dr. Dwayne Hodges, USA, (Ret.)

CISSP, CCISO, CEH, CNDA, ECES, SEC+ ITIL

# Advanced Asymmetric Cryptography Concepts

- Goals of Cryptography
  - Confidentiality
  - Integrity
  - Availability
  - Non-Repudiation

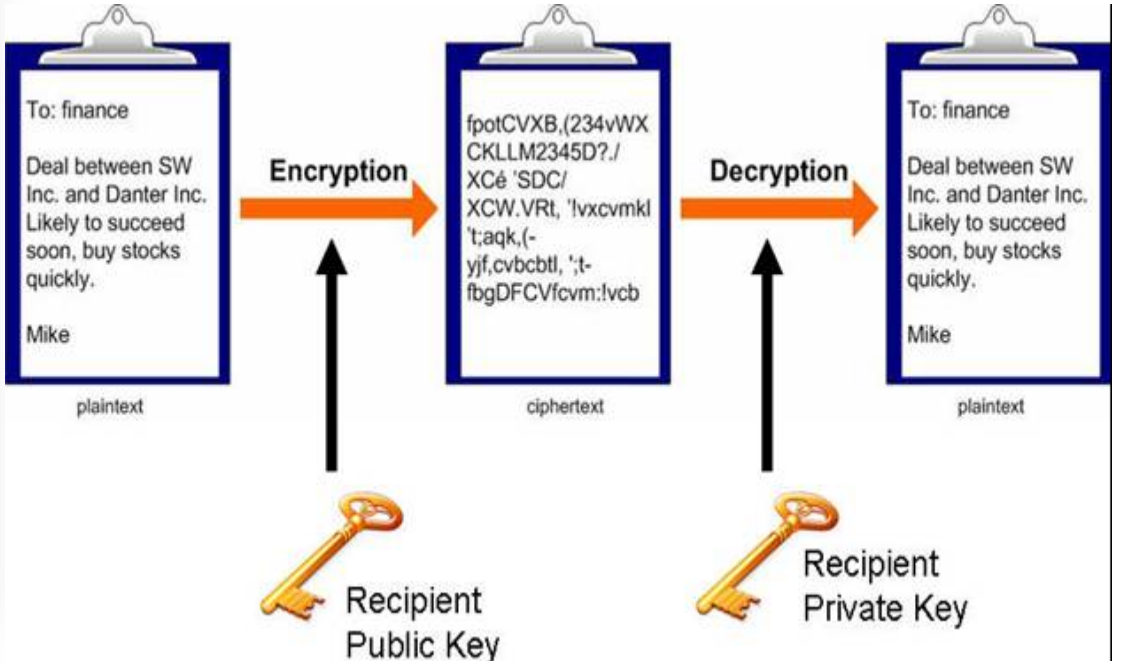
# Advanced Asymmetric Cryptography Concepts

- Based on mathematical number theory
- Each user has two keys: Public/Private
  - Public key is available to everyone
  - Private key is kept secret
- Both keys are mathematically related
  - Considered a key pair, Private and Public
  - Whatever is encrypted with one key, can only be decrypted with the other

# Advanced Asymmetric Cryptography Concepts

- Based off discrete mathematical operations in the finite field
- Based on a one-way function ( trap door)
  - Easy in one way, impossible the other way
- Used for encryption and signatures
- Provided confidentiality, authentication, and Non-repudiation
- strong key distribution
- High scalability, however slower than symmetric
- Suitable for small amount of data

# Advanced Asymmetric Cryptography Concepts

# Advanced Asymmetric Cryptography Concepts

- Zero proof knowledge
  - your private key encryption can be proofed with your public key
- Open message security format
  - Message secured with user's private key
- Secured message format
  - Message secured will recipient's public key

# Advanced Asymmetric Cryptography Concepts

Advantages

- Key Management
- Public key can be freely distributed
- Offers: Digital signatures, integrity checks, key exchange, and non-repudiation

Disadvantages

- Typically 100 to 1000 times slower than symmetric key algorithms
- The resulting file size of an encryption is larger


# Advanced Asymmetric Cryptography Concepts

## RSA (Rivest, Shamir, Adleman)

- Encryption, Digital Signatures, Key Exchange, Key distribution
- Based on the difficulty of factoring two large numbers into their original **prime numbers**
- Variable Block and Key length
  - 512-bit to arbitrarily long
  - 1024-2048 considered secure
  - 8000 >
- Used in several applications
  - E-commerice, banking, VISA, Bluetooth, TLS, PGP,

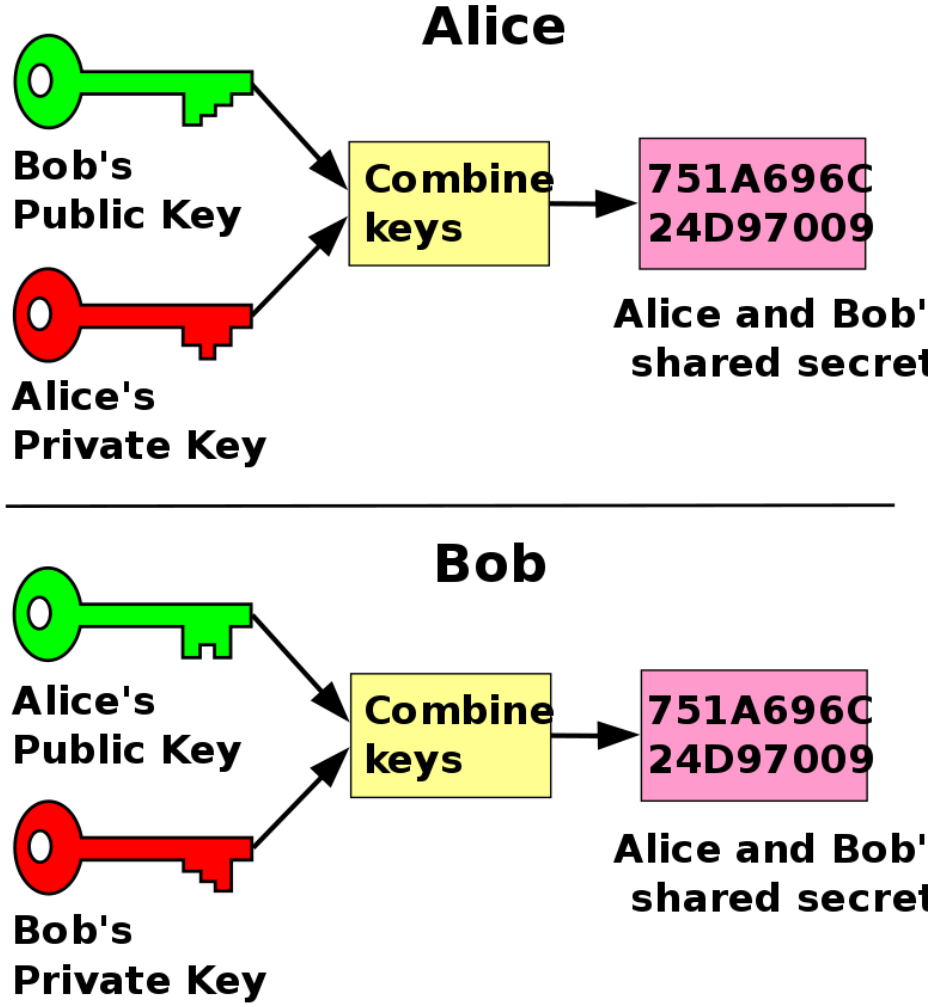
# Advanced Asymmetric Cryptography Concepts

- ECC (Elliptic Curve Cryptography)
  - Encryption, Digital Signatures, Key Exchange/agreement
  - Allows for smaller keys
  - Endorsed by NSA as Suit B
  - Based on the idea of using points on  a curve to define the public/private key
    - Requires less computing power
  - An ECC key of 256-bits is equivalent to 3072 RSA public key
  - Implemented on hardware devices such as wireless devices and smart cards
  - Vulnerable to quantum attacks

# Advanced Asymmetric Cryptography Concepts

- Diffie-Hellman
  - Provides for Key Exchange
  - Based on the difficulty of computing discrete logarithms
  - Variable key length
    - 512-bit to arbitrarily long
    - 1024-2048 considered secure
  - About the same strength as a 3072-bit RSA key
  - Used in PGP
  - Private and Public keys are generated
  - Session key is created
  - Session key is shared
  - Vulnerable to MITM

# Advanced Asymmetric Cryptography Concepts



# Advanced Asymmetric Cryptography Concepts

El Gamal

Encryption, Digital Signatures, Key Exchange

Based upon the Diffie-Hellman

Main drawback is performance (slower than other comparable algorithms)

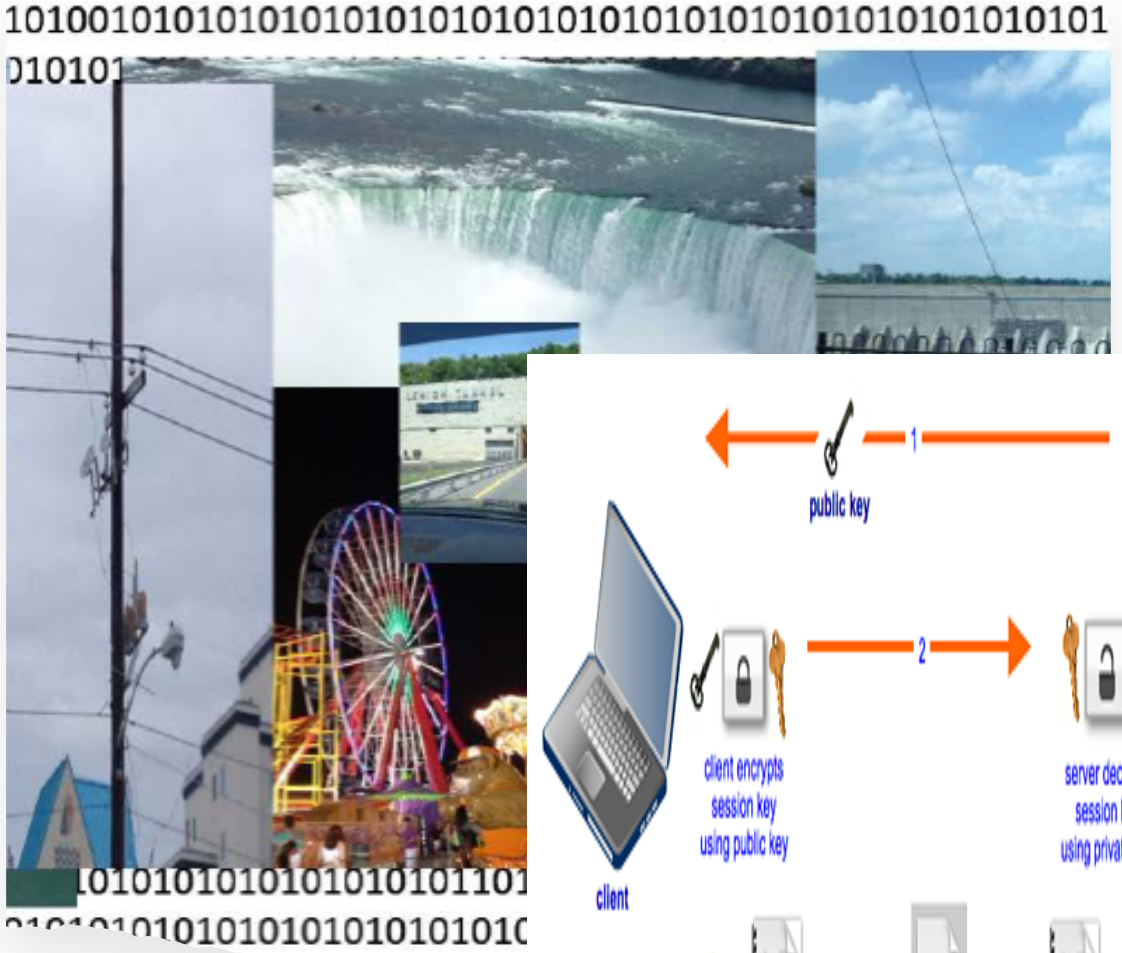
DSA (Digital Signature Algorithm) provides authentication, integrity, and non-repudiation working within a crypto syster

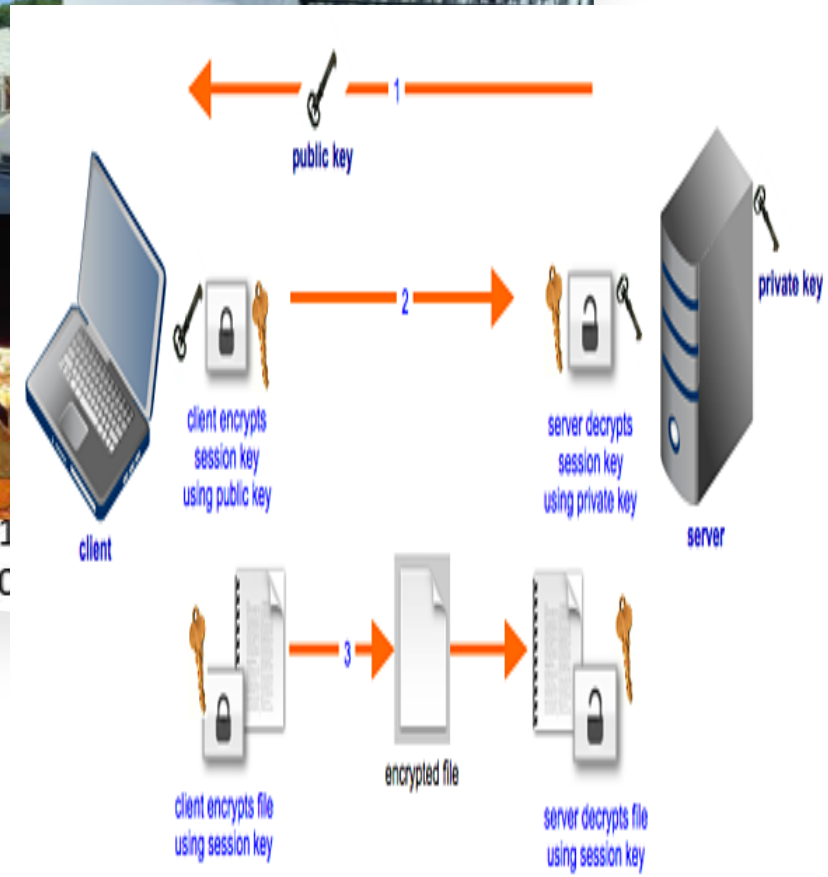
Used to digitally sign documents

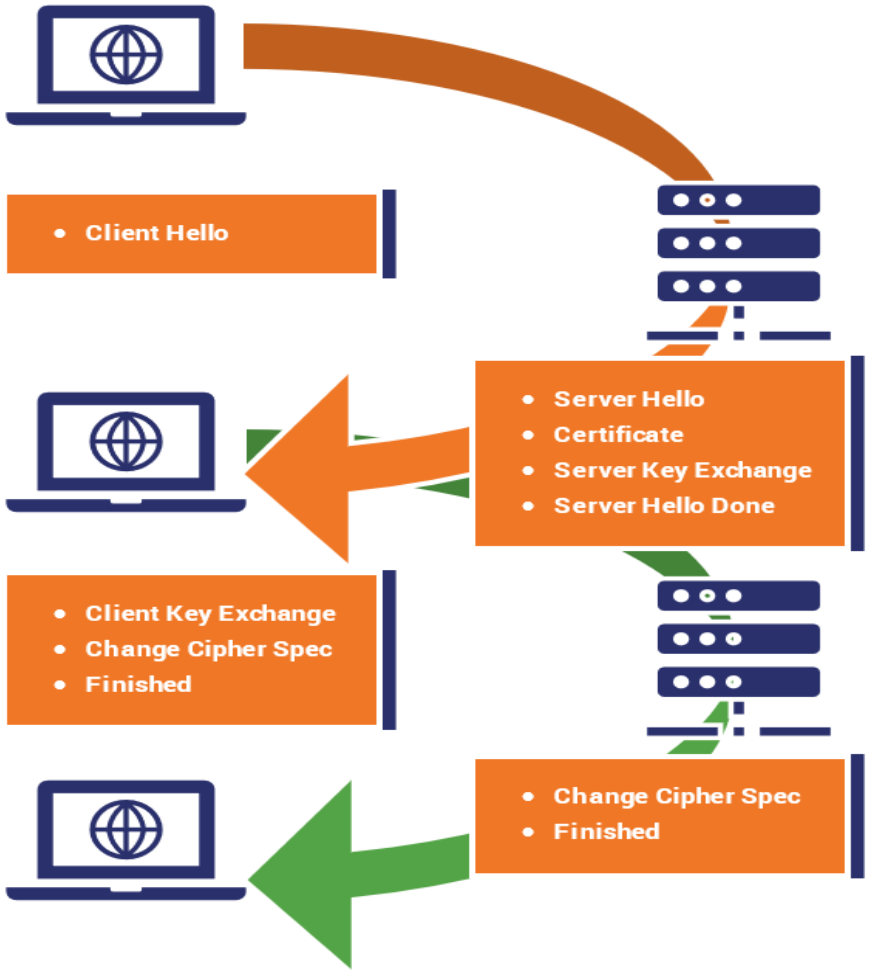
- Private key signs
- Public key verifies
- Provides message authentication

Performs an integrity check by use of SHA-1

# Advanced Asymmetric Cryptography Concepts



# Advanced Asymmetric Cryptography Concepts

| | | |
|---|---|---|
| **RSA** | Leverages prime number characteristics, 1024- 8000 bit variable key size, 1 round | Most Popular / provides authentication and encryption / authentication through digital signatures |
| **ECC** | Leverages discrete logarithm characteristics | provides authentication and encryption/ faster than RSA / Uses less resources than RSA (Used in smaller devices like smartphones) / authentication through digital signatures |
| **El Gamal** | Used in recent versions of PGP | Extension of Diffie Hellman (DH)/ Similar level of protection as RSA an ECC/ usually the slowest |
| **Knapsack** | Used for encryption only at first | Consider insecure |
| **DSA** | Used to verify signatures, used Key pair, verified with ” public key” | FIPS -186 Standard |
| **Diffie Hellman (DH)** | No Authentication /vulnerable to Man in the middle attacks | |