Data Security

HUM4441

Dr. Mohammad Rezwanul Huq

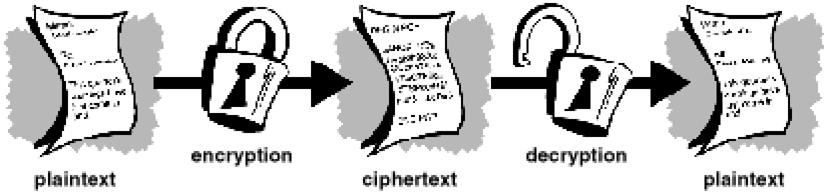
Encryption And Decryption

Encryption Terminology

- *Encryption*: Transform representation so it is no longer understandable
- *Cryptosystem*: A combination of encryption and decryption methods
- *Cleartext* or *Plaintext*: Information before encryption
- *Cipher text*: Information in encrypted form
- *One-way cipher*: Encryption system that cannot be easily reversed (used for passwords)
- *Decryption*: Reversing encryption process

Encryption And Decryption

- To ensure the privacy of messages sent over a network between a source and destination, the text can be encrypted.
  - **Cryptography** - study of methods to encrypt text.
  - **Cryptanalysis** - study of how to decode an encypted text.



- **Conventional or single key encryption** - a simple algorithm is used to transform the text
  - **substitution cipher** - each letter of the alphabet is substituted with a different letter or symbol.
  - **Ceasar's method** - replace every letter in the alphabet with the letter 3 away

A - > D

B - > E

C - > F

. . .

X - > A

Y - > B

Z - > C

Encryption And Decryption

- Other substitution ciphers assign random substitutions, so they are a bit harder to crack.
  - The sender uses the encryption to encrypt the message
  - The sender transmits the message to the receiver
  - The receiver decodes the message

- How does the receiver decode the message? The sender needs to send the key to the receiver.
  - How can this be done securely so that no one else can decode the message?
  - To secure e-commerce transactions on the Web, the buyer's machine must encrypt the data before it sends it over the Internet to the merchant's Web server

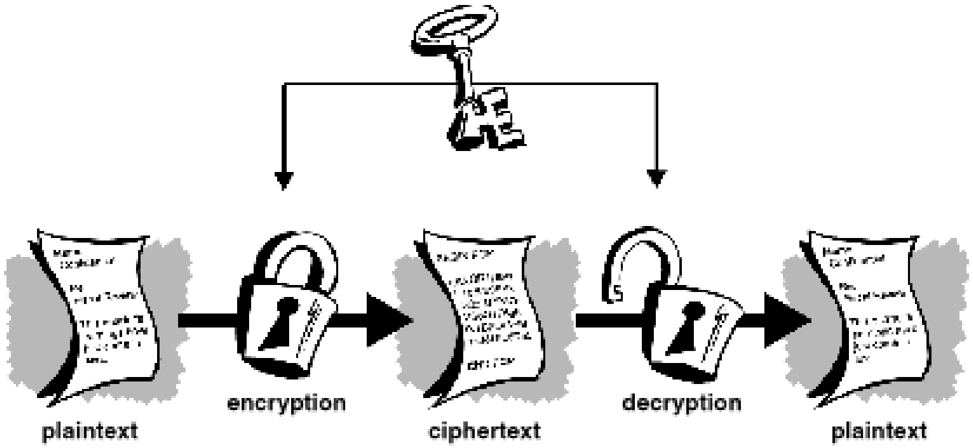
Encryption And Decryption

- Most encryption algorithms use mathematical formulas and an encryption key to encode the data
  - The encryption key is a very large number used to encrypt and decrypt the data
  - The length of the key (the number of digits it contains) determines how secure the data will be – the longer the key the more secure the message
  - Most encryption algorithms use key length between 40 and 128 bit or more
    - Most Web browsers support these length keys

Encryption And Decryption

Symmetric/ Private Key Encryption

- Uses a single number key to encode and decode the data. Both the sender and receiver must know the key
- DES (Data Encryption Standard) is the most widely used standard for symmetric encryption
- Because each sender and receiver would require a different key, this type of encryption is basically used by government entities
- It is rarely used for e-commerce transactions over the Internet
- Requires a secure way to get the key to both parties



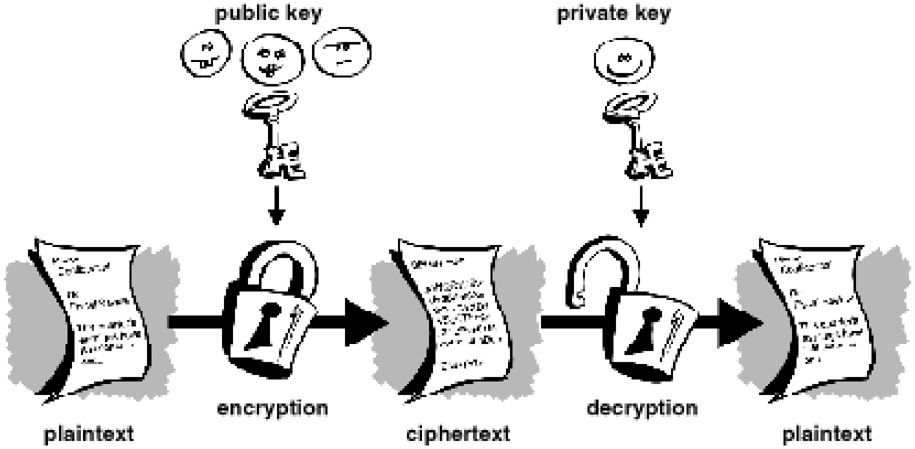
Encryption And Decryption

Asymmetric / Public Key Encryption

- Uses two numeric keys
  - The public key is available to anyone wishing to communicate securely with the key's owner
  - The private key is available only to the owner
- Both keys are able to encrypt and decrypt each other's messages
- It is computationally infeasible to deduce the private key from the public key. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information.
- Example: encode by raising to 5th power and moding result with 91

Decode by raising to 29th power mod 91

$32^5 = 2 \pmod{91}$ and $2^{29}=32 \pmod{91}$



Assymetric Encryption

- Choose two large prime numbers, p and q and compute $N = p * q$ and $x = (p-1)*(q-1)$
- Choose a number relatively prime to x and call it e. This means that e is not a prime factor of x or a multiple of it.
- Find d such that $e * d = 1 \bmod x$.

  To encrypt: $Cipher = Plaintext^e \pmod n$
  To decrypt: $Plaintext = Cipher^d \pmod n$

- Choose $p = 7$ and $q = 13$
- We then calculate $N = 7*13 = 91$ and $x=(p-1)(q-1) = 72$
- We next select k_e relatively prime to 72 and< 72, yielding 5
- Finally,we calculate k_d such that $k_e k_d \bmod 72 = 1$, yielding 29
- public key $(k_{e,} N) = (\mathbf{5}, 91)$ and private key $(k_d, N) = (\mathbf{29}, 91)$

32 codes in 2: $32^5 = 2 \pmod{91}$

2 decodes into 32: $2^{29} = 32 \pmod{91}$

Encryption And Decryption

Asymmetric / Public Key Encryption

- The primary benefit of asymmetric cryptography is that it allows people who have no preexisting security arrangement to exchange messages securely.
- The need for sender and receiver to share secret keys via some secure channel is eliminated
    - all communications involve only public keys, and no private key is ever transmitted or shared.
    - Some examples of public-key cryptosystems are
        - Elgamal (named for its inventor, Taher Elgamal)
        - RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman)
        - Diffie-Hellman (named, you guessed it, for its inventors)
        - DSA, the Digital Signature Algorithm (invented by David Kravitz).
        - PGP (Pretty Good Privacy) is fairly popular and inexpensive
- Because conventional cryptography was once the only available means for relaying secret information, the expense of secure channels and key distribution relegated its use only to those who could afford it, such as governments and large banks
- Public key encryption is the technological revolution that provides strong cryptography to the public

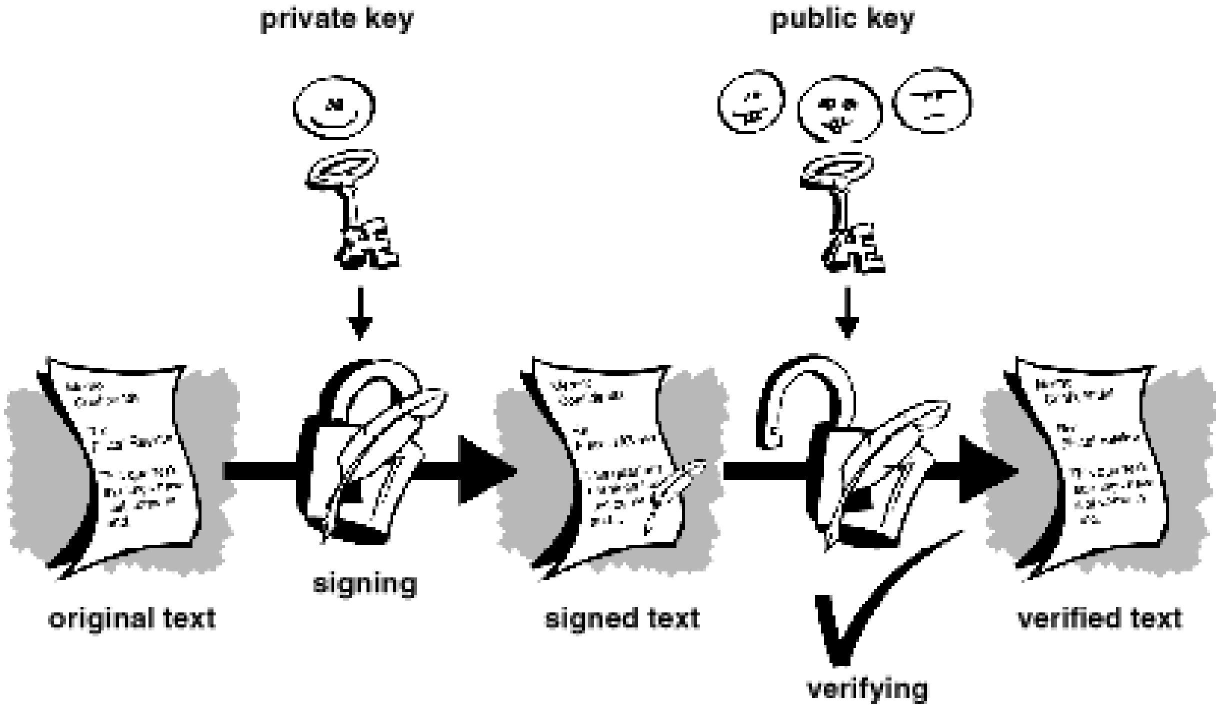
Digital Certificates

Digital Certificates

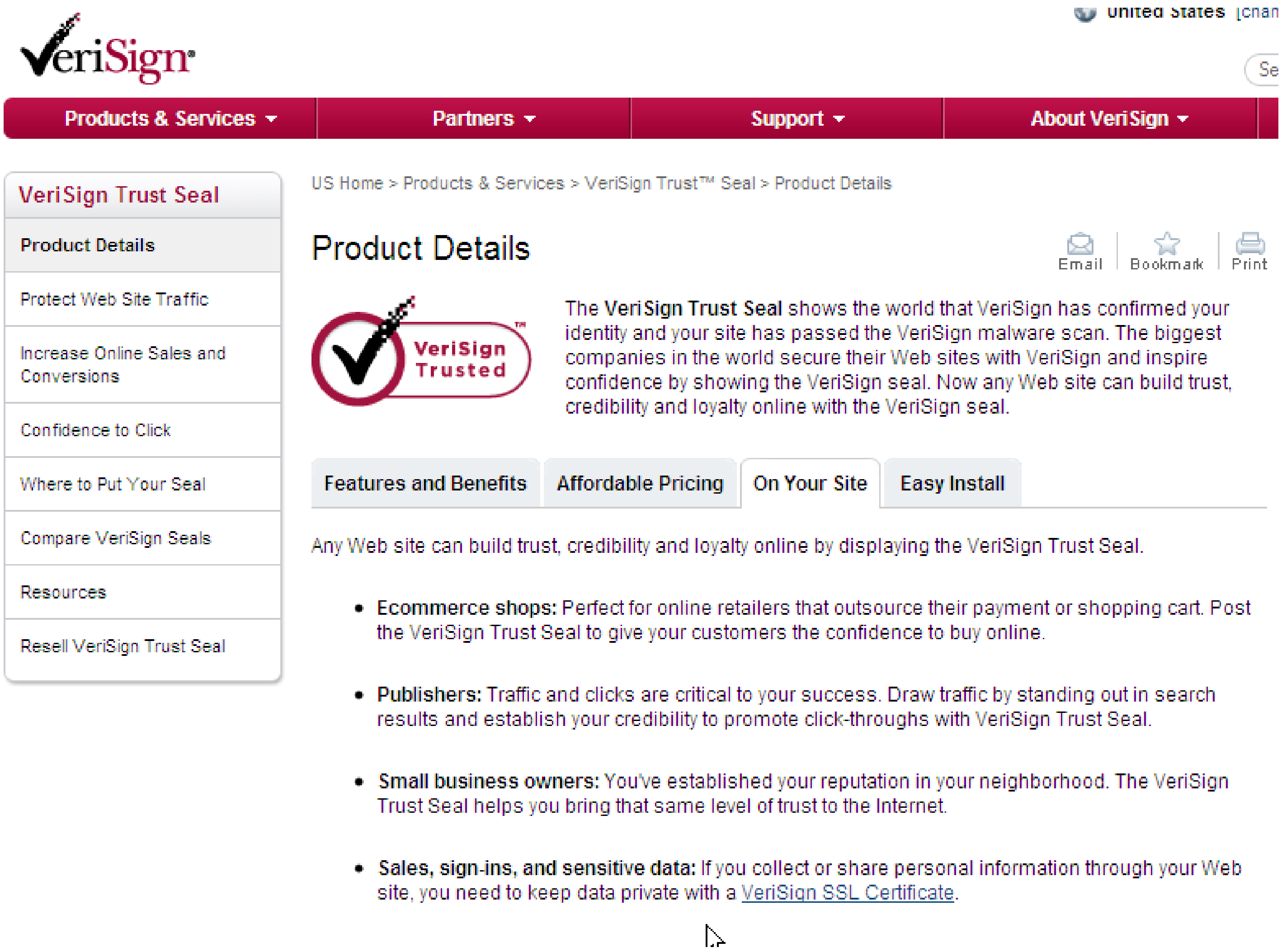
- Use assymetric encryption to create digital signatures
- Used on the Internet to authenticate both users and vendors
- A digital certificate is a unique identifier assigned to a user/vendor by a certification authority to verify the identity of the user/vendor
  - A certification authority (such as VeriSign) is a private company that certifies the user or vendor is who s/he claims to be
  - Work together with credit card verification companies or other financial institutions in order to verify the identity of the certificate's requesters
- Digital signature is an encrypted attachment added to the electronic message to verify the sender's identity
  - The digital certificate received by the user includes a copy of its public key
  - This digital certificate's owner makes its public key available to anyone wanting to send encryped documents to the certificate's owner

Digital Signatures

- Instead of encrypting information using someone else's public key, you encrypt it with your private key. If the information can be decrypted with your public key, then it must have originated with you.



VeriSign – certification authority



Product Details

The **VeriSign Trust Seal** shows the world that VeriSign has confirmed your identity and your site has passed the VeriSign malware scan. The biggest companies in the world secure their Web sites with VeriSign and inspire confidence by showing the VeriSign seal. Now any Web site can build trust, credibility and loyalty online with the VeriSign seal.

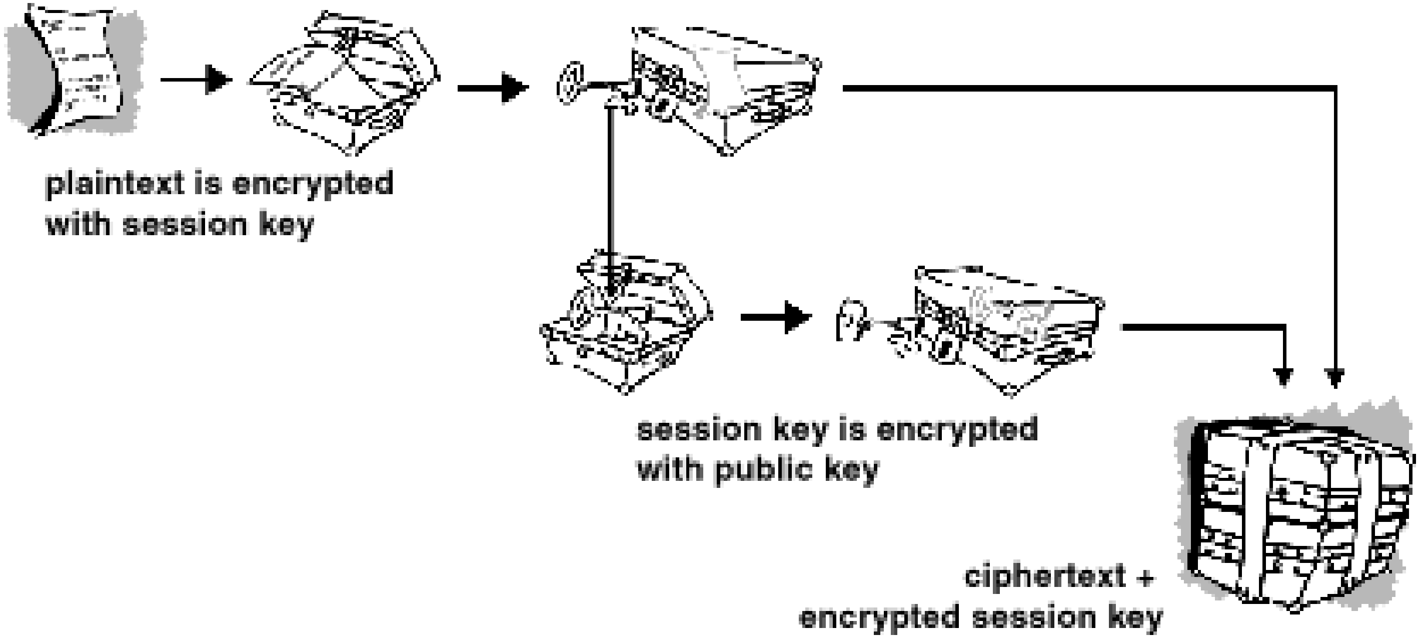
Any Web site can build trust, credibility and loyalty online by displaying the VeriSign Trust Seal.

- **Ecommerce shops:** Perfect for online retailers that outsource their payment or shopping cart. Post the VeriSign Trust Seal to give your customers the confidence to buy online.
- **Publishers:** Traffic and clicks are critical to your success. Draw traffic by standing out in search results and establish your credibility to promote click-throughs with VeriSign Trust Seal.
- **Small business owners:** You've established your reputation in your neighborhood. The VeriSign Trust Seal helps you bring that same level of trust to the Internet.
- **Sales, sign-ins, and sensitive data:** If you collect or share personal information through your Web site, you need to keep data private with a VeriSign SSL Certificate.

How PGP Works – Encryption

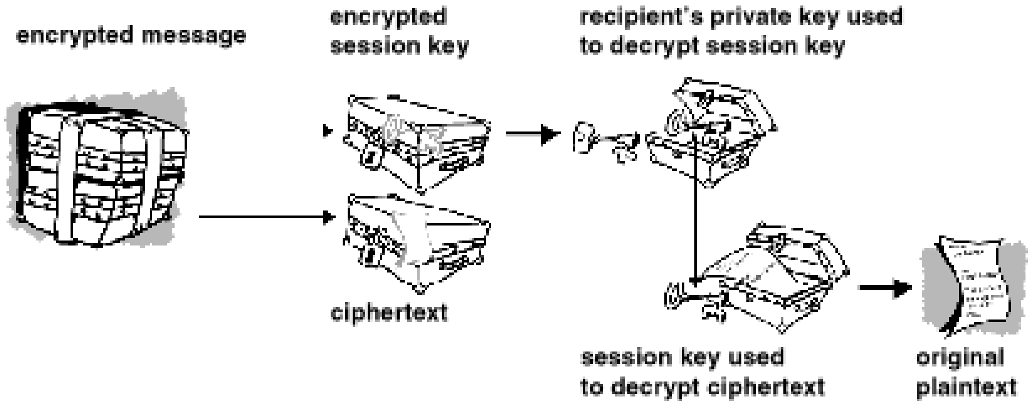
- PGP combines some of the best features of both conventional and public key cryptography; it's a *hybrid cryptosystem.*
- When a user encrypts plaintext with PGP, PGP first compresses the plaintext.
  - Data compression saves transmission time and disk space and, more importantly, strengthens cryptographic security.
    - Most cryptanalysis techniques exploit patterns found in the plaintext to crack the cipher. Compression reduces these patterns in the plaintext, thereby greatly enhancing resistance to cryptanalysis.
  - PGP then creates a *session key,* which is a one-time-only secret key.
    - This key is a random number generated from the random movements of your mouse and the keystrokes you type.
    - This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext.
    - Once the data is encrypted, the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient.

How PGP Works – Encryption



How PGP works – decryption

- Decryption works in the reverse. The recipient's copy of PGP the private key to recover the temporary session key, which PGP then uses to decrypt the conventionally-encrypted ciphertext.


encrypted message
encrypted session key
recipient's private key used to decrypt session key
ciphertext
session key used to decrypt ciphertext
original plaintext

- The combination of the two encryption methods combines the convenience of public key encryption with the speed of conventional encryption. Conventional encryption is about 1, 000 times faster than public key encryption. Public key encryption in turn provides a solution to key distribution and data transmission issues. Used together, performance and key distribution are improved without any sacrifice in security.