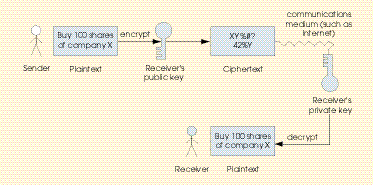
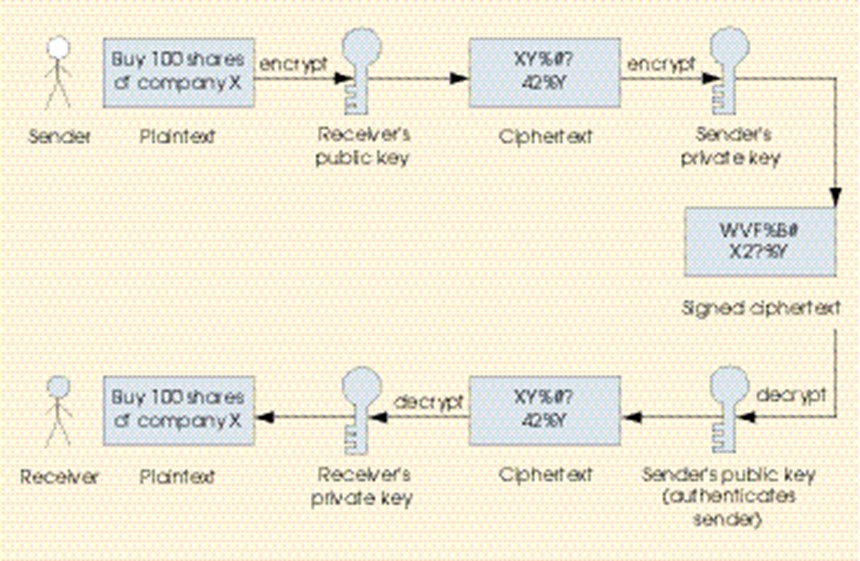
**Explain about Public key cryptography**

* Cryptography
  + Transforms data using cipher or cryptostream
  + Key acts as password that combined with cipher will decrypt encoded message into original message
  + Early cryptography relied on symmetric cryptography
    - Same key used to encrypt and decrypt
    - Problem of how to securely transmit key itself arose
  + Solution was public-key cryptography
    - Two related but different keys used
    - Sender uses receiver’s public key to encode
    - Receiver decodes with private key
    - Keys long enough that guessing or cracking them takes so much time it is not worth the effort

**Encrypting and decrypting a message using public-key cryptography.**



* Digital signatures
  + Same concept as physical written signatures
    - Authenticate signer
    - Difficult to forge
  + Part of public-key cryptography
  + Generated by running phrase through hash function
    - Returns hash value
  + Hash value for a phrase is over 99% guaranteed unique
    - ie., two different phrases very unlikely to generate same value
* Authentication with a public-key algorithm.



* PKI implementations
  + More secure than standard point-of-sale (POS) transactions
    - Strong encryption can take decades to crack using current technology
  + RSA encryption popular choice for PKI
    - Developed at MIT in 1977
  + Pretty Good Privacy (PGP)
    - Implementation of PKI
    - Very popular way to encrypt e-mail
    - Operates using web of trust

**Explain microsoft IIS.**

* Internet Information Server (IIS)
  + Extends Windows NT server to Intranets and Internet
  + Provides full Intranet and Internet Web capabilities
  + Publish information
  + Access to data stored in various client/server databases
  + Supports CGI
    - CGI creates separate process for every request
    - Microsoft alternative: ISAPI
  + Back-end database access and programming
    - IDC connects to back-end ODBC databases
      * Insert, update, delete, etc.
* Internet Service Manager
  + GUI manager

**Explain about Apache and Jigsaw web server**

* Apache
  + Leading UNIX Web server
  + High-performance httpd (HTTP daemon) server
    - *Daemon*: UNIX background process that implements server side of a protocol
  + Server-side programming tools and languages:
    - Perl
    - PHP3
      * Scripting language that allows embedding scripting code into HTML pages
    - Tcl
    - Python
  + Access to Java Servlet API
  + JSP (JavaServer Pages)
    - Embed java code within HTML templates 🡪 dynamic pages processed entirely by server

Modules provide additional functionality

* + - <http://modules.apache.org/>
    - **mod\_SSL**
    - Strong cryptography for Apache 1.3 Web server via Secure Sockets Layer
    - **mod\_perl**
    - Modules can be written entirely in Perl
    - **Jserv**
    - Module that implements Sun’s Java Servlet API

On Windows NT

* + - Apache Web server run as console application or service
    - *Console application*: stopping and starting server is manual
    - *Service*: Apache starts whenever operating system starts