Posters:
- size should not exceed 4’x3’ electronic copy must be submitted by Wed, Dec 6th at 9am
- printing can be done for free at CNS computer lab in anatomy-zoology building E100
- If there are issues printing in E100, please seek an account number from Dr. Ray before printing at the Morgan Library.
- presentations on Dec 7th from 9:30 to 11:30.
- PDF of the project due Dec. 6th by 9am.
- Template should be posted (Friday 12/1)

S/MiMe
- can be used for secure email, EDI,
  - better than https to connect to gmail we secure the email during transit to gmail server but we don't know how it is stored
  - Designed for large files such as images and binary files
  - Does not guarantee the delivery recipient but is confidential
  - Digital Signature Standard

SMIME has lots of security guarantees that https does not have
- SMIME provides enveloped data, signed data, clear signed data, signed and enveloped data
- encryption with public key tech and digital signature
- Can't use a public key for very large files as it is very slow
- create one-time session key encrypt the message

Process
- take the plaintext message, add a digital signature, message with a signature encrypted, encrypted copy of session key added, doc converted to radix-64
  1. Plaintext message created
  2. Digital signature added (DSS/SHA)
  3. Message with signature encrypted with one time session key (Triple DES)
  4. Encrypted copy of session key added (El Gamal)
  5. Document converted to Radix-64 format
  6. Receiver decrypts session key using private key
  7. Receiver decrypts message with session key

different variants for how SMIME can be performed
- we can make the message with the sender using their private key first, then use the receiver’s public key
- the sender can also use the receiver’s public key first then their private key
- there is a difference and the better option has to do with what the sender and receiver think are the best option
  - in the first case, the signature (sender private key) is hidden by the encryption technology
  - in the second case you sign an encrypted message
  - the choice to use one or the other has to do with the type of threat you encounter
as new types of SMIME come out new techniques and standards are added

- new signature
- to encrypt an outgoing message
  - SMIME does not let you send message to groups
  - SMIME needs to obtain a valid certificate for each and every member of the group
  - Group keys can be made, but are not specifically managed by SMIME
- has effective encryption and signature services
- maintains public keys
- each client has a list of trusted CA certificates and own public-private key pairs and certificates

S/Mime Certificates
- Sender must have certificate to sign outgoing messages
- Need to use a key management utility and certificate management program when communicating with multiple entities. S/Mime does not support these.

transport layer security provides protection during transit, but we don't know what happens when it reaches the destination

- sockets layer is an interface between the application layer and the transfer layer.
- sock layer hides the details of how the process works but it allows the application to access all the lower layers.
- use TCP for reliable end to end service
- may be provided in underlying protocol suite or embedded in specific packages
- Sockets Layer allows app developers to hide details of how packet will be handled. SSL protocol or TLS protocol allows developers to use the Sockets Layer.
- Do not provide security while the data is in rest, protects only during transit.
- Ensures edge to edge security – endpoint to endpoint.

SSL/TSL Goals
- Integrity is strongly protected
- No guarantee about storage security
- Cryptographic security, Interoperability, Extensibility, Relative efficiency (measured in bandwidth usage)

the SSL handshake protocol interacts directly with the TCP protocol. It begins with an insecure channel, then at the end of the SSL handshake, it creates a secure tunnel between who is interacting and hands off to the SSL record protocol.

-SSL Record Protocol Services
  - Applies Compression Techniques to increase efficiency
  - Adds message authentication code using secret key identified during handshake
  -Provides secure tunnel
    - message integrity done with MAC with shared secret key
    - like HMAC but with different padding
    - confidentiality done with symmetric encryption with a shared secret key defined by handshake protocol
    - message is compressed before encryption
  -operation:
1. App data in original form
2. Fragmented into parts
3. Each part is compressed
4. Add MAC
5. Encrypt (with symmetric key established in handshake protocol)
6. Append SSL record header
7. Message given to transport layer

-SSL Alert Protocol
  -conveys SSL-related alerts to peer entity
  -severity: warning or fatal
  -specific alert:
    Fatal - unexpected message, bad record mac, decompression failure, handshake failure, illegal param (exits connection)
    Warning: close notify, no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown - there can be problems with certificates, allows user to handle problem

When the SSL record protocol breaks up the application data into fragments, how does it deal (compress and add the mac) with possible remaining data that does not have the correct fixed size?

Padding

How does using the one-time session key make S/MIME more secure than just using the receiver's public key for encryption?

The session key changes, it would be harder to brute force.

How is S/MIME protocol compared to using PGP encryption with popular email service such as Gmail?

SMIME requires a certificate server

how much does the SSL protocol differ from other protocols in terms of speed?

Not much
How exactly do compression techniques find patterns in messages? Are they optimal?

Look for common sequences, encode those sequences as a shorter sequence, different compression techniques will yield different results.

In the S/MIME process, does Alice (as the recipient) use a private key or any particular resource that allows only her to decrypt the message?

Yes, a private key