Please provide the raw text content that needs to be converted into a natural language representation.
for symmetric encryption of messages
- Asymmetric encryption algorithms
  - RSA = block cipher
  - currently uses 1024 bit key

**Digital Signatures**

- bob creates message, generates hash value for the message, and encrypts hash code with private key, creating a digital signature
- alice receives messages plus signature
  - recalculates hash value for message
  - decrypts signature using bobs public key
  - compares calculated hash value to decrypted hash value
- the message is safe from alteration, but not from observation

**Certificates**

- downside: some user could send their public key, purporting to be Bob.
- solution is public key certificate
  - consists of public key, userid, plus signed by trusted 3rd party (ie verisign)