**Safe Data Transfer**  
**краткий пересказ**

Secure transactions across the Internet have three goals. First, the two parties engaging in a transaction (say, an email or a business purchase) don't want a third party to be able to read their transmission. Some form of data encryption is necessary to prevent this. Second, the receiver of the message should be able to detect whether someone has tampered with it in transit. This calls for a message-integrity scheme. Finally, both parties must know that they're communicating with each other, not an impostor. This is done with user authentication. Today's data encryption methods rely on a technique called public-key cryptography. Everyone using a public-key system has a public key and a private key. For the system to work, two parties engaging in a secure transaction must know each other's public keys. Private keys, however, are closely guarded secrets known only to their owners. To make a message tamper-proof (providing message integrity), the sender runs each message through a message-digest function. This function within an application produces a number called a message-authentication code (MAC). The system works because it's almost impossible for an altered message to have the same MAC as another message. Also, you can't take a MAC and turn it back into the original message. The dynamics of the Web dictate that a userauthentication system must exist. This can be done using digital certificates. A server authenticates itself to a client by sending an unencrypted ASCII-based digital certificate. A digital certificate contains information about the company operating the server, including the server's public key. The digital certificate is 'signed' by a trusted digitalcertificate issuer, which means that the issuer has investigated the company operating the server and believes it to be legitimate.