Lecture 8
Internet Security

Lecturer: Professor Rasulev D.M.

Internet Security

- basic concepts of security
- public-key/private-key cryptography
- security protocols
- digital signatures, digital certificates
- and certification
- secure systems
- emerging security techniques

Internet Security

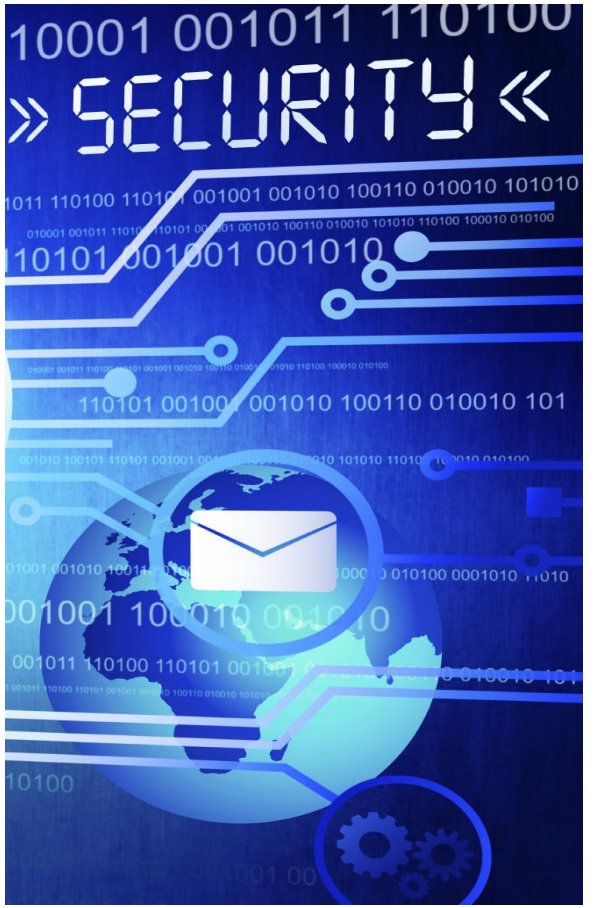
Ancient Ciphers to Modern Cryptosystems

Cryptography transforms data

Ciphertext

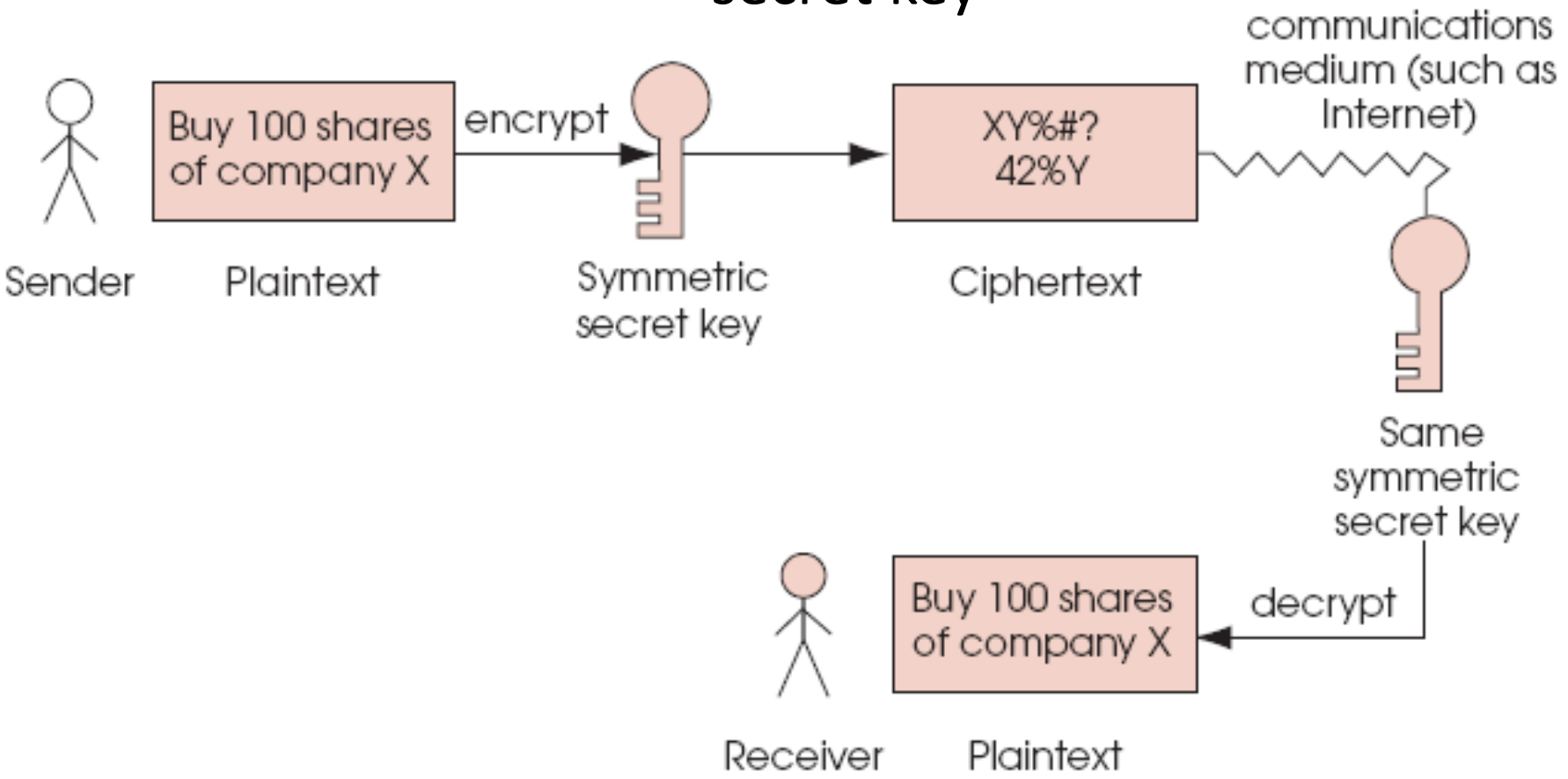
Encrypt to “tfdvsjuz

Digital



Secret-key Cryptography

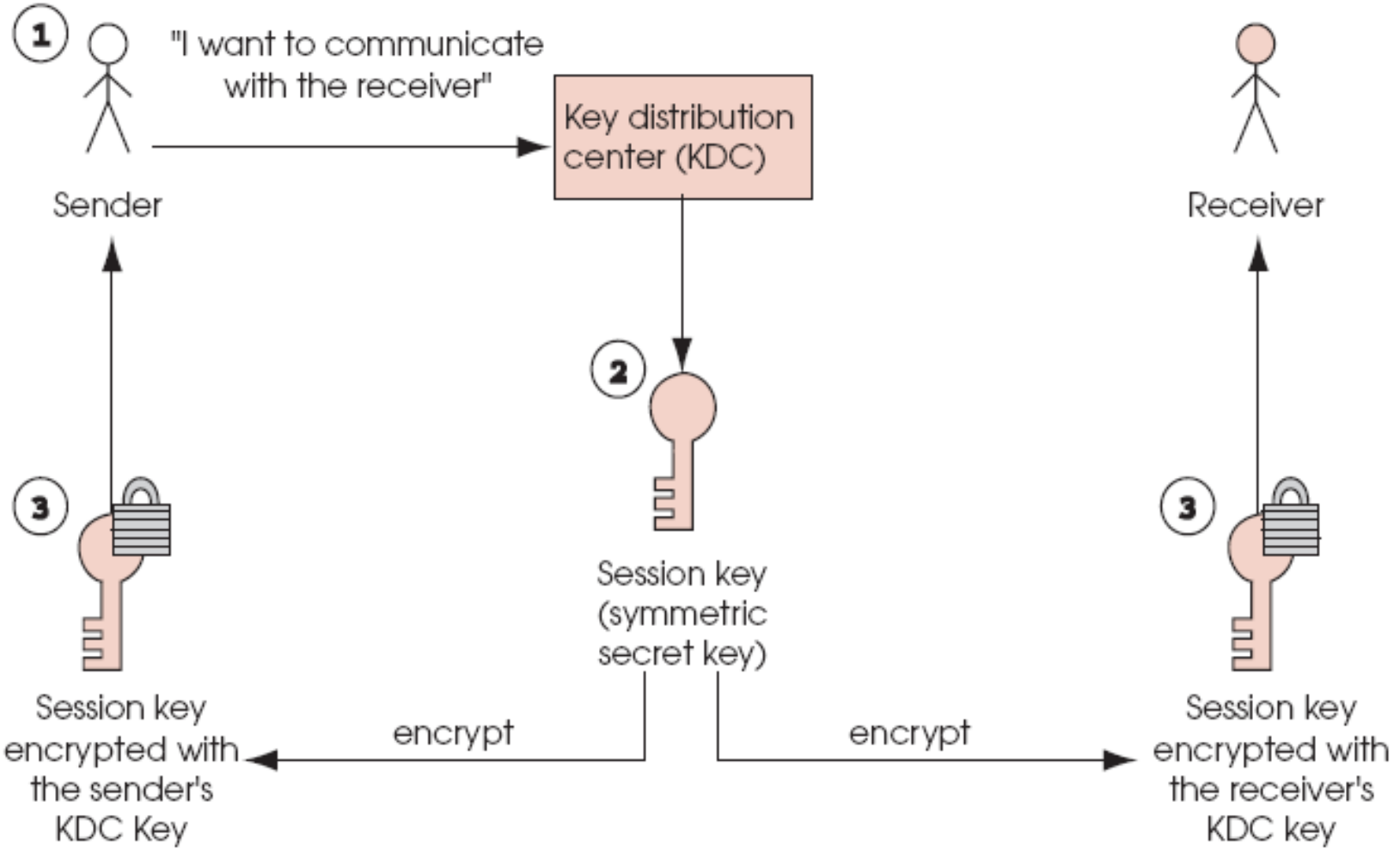
Encrypting and decrypting a message using a symmetric secret key



Source: E-Business and e-commerce for managers, H. M. Deitel, P. J. Deitel, K. Steinbuhler, Prentice Hall, 2011

Secret-key Cryptography

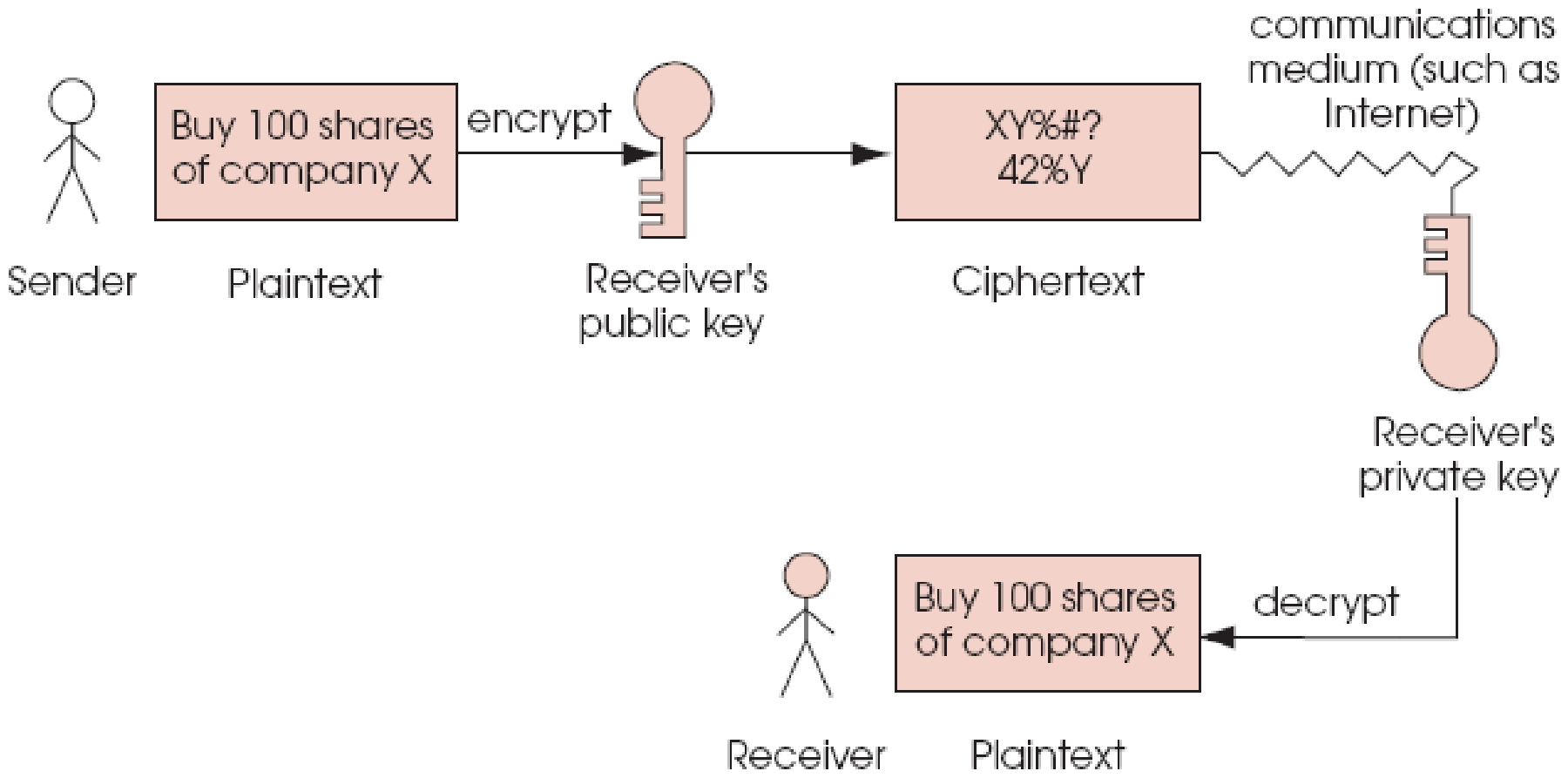
Distributing a session key with a key distribution center.



Source: E-Business and e-commerce for managers, H. M. Deitel, P. J. Deitel, K. Steinbuhler, Prentice Hall, 2011

Public-key Cryptography

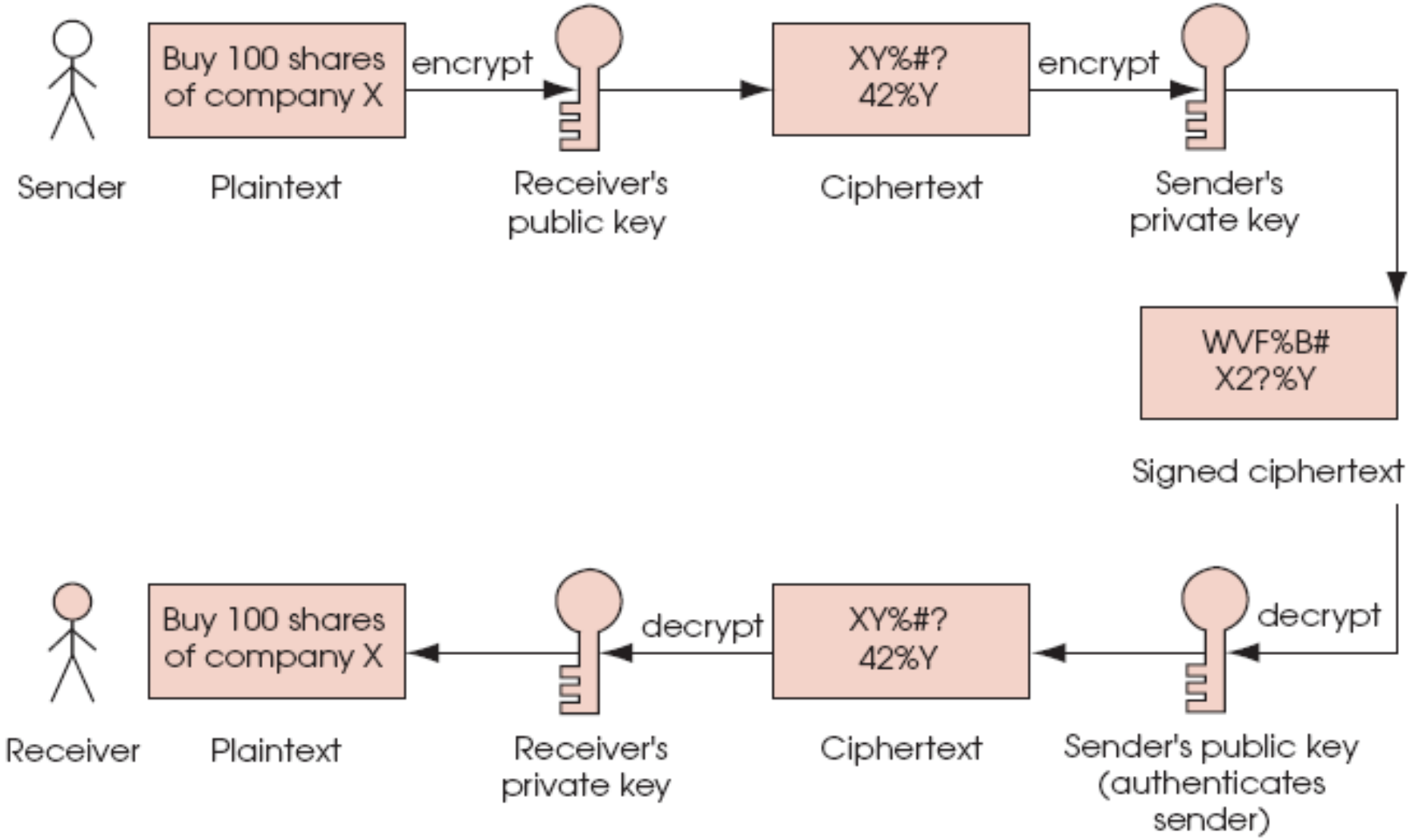
Encrypting and decrypting a message using public-key cryptography.



Source: E-Business and e-commerce for managers, H. M. Deitel, P. J. Deitel, K. Steinbuhler, Prentice Hall, 2011

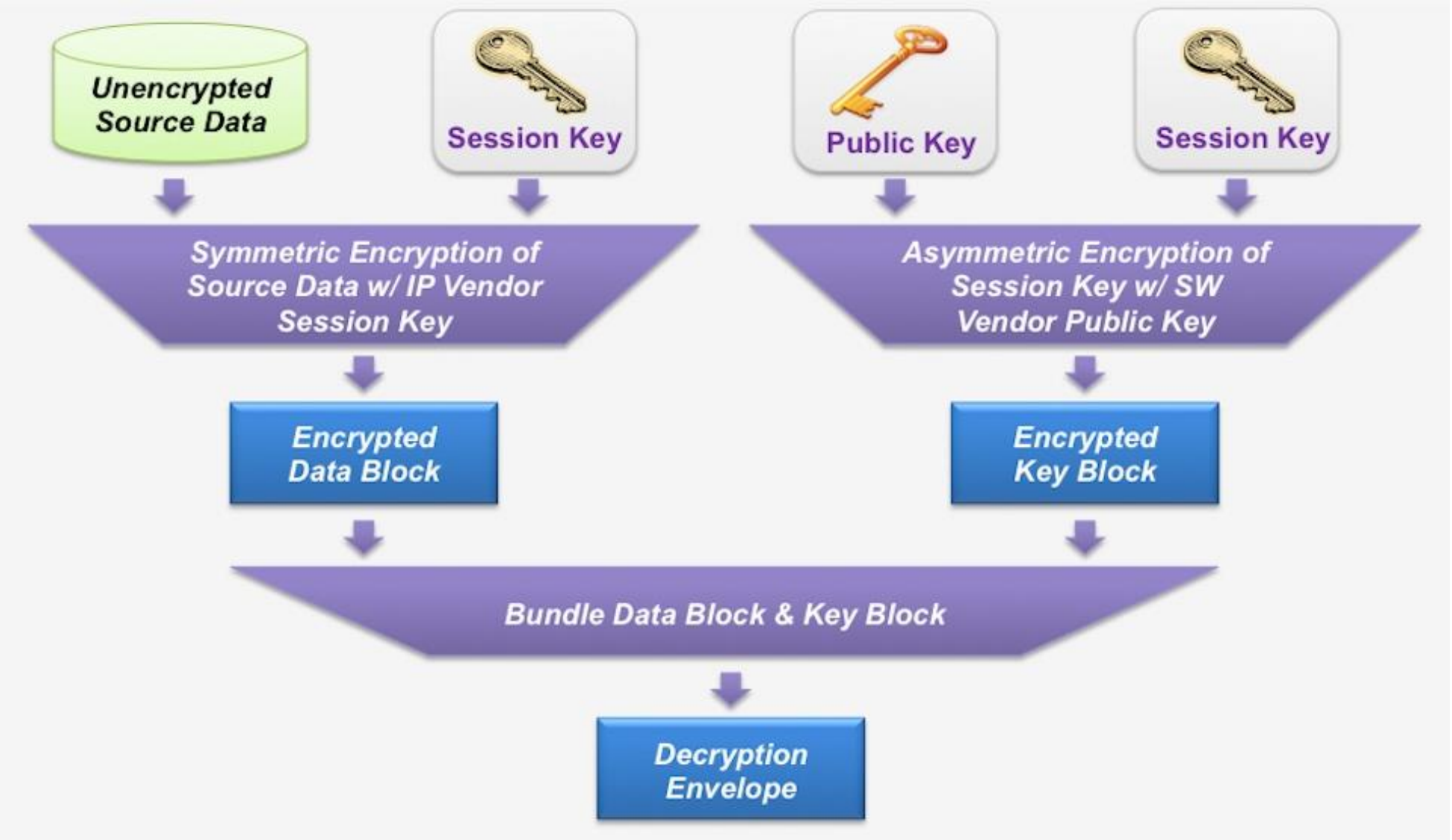
Public-key Cryptography

Authentication with a public-key algorithm.



Source: E-Business and e-commerce for managers, H. M. Deitel, P. J. Deitel, K. Steinbuhler, Prentice Hall, 2011

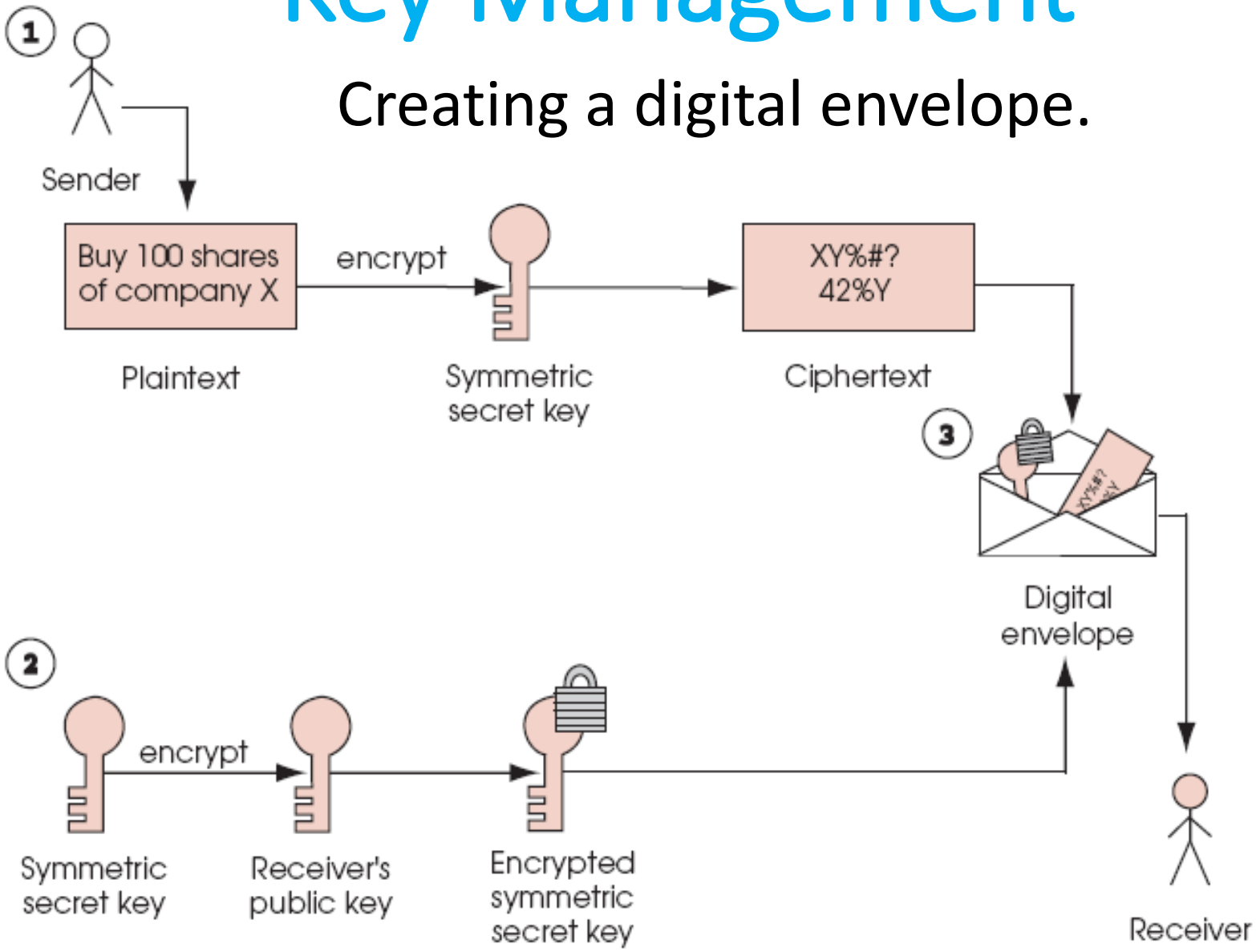
Key Agreement Protocols



Source: http://www.techdesignforums.com/practice/technique/ip-based-fpga-design-synplify/

Key Management

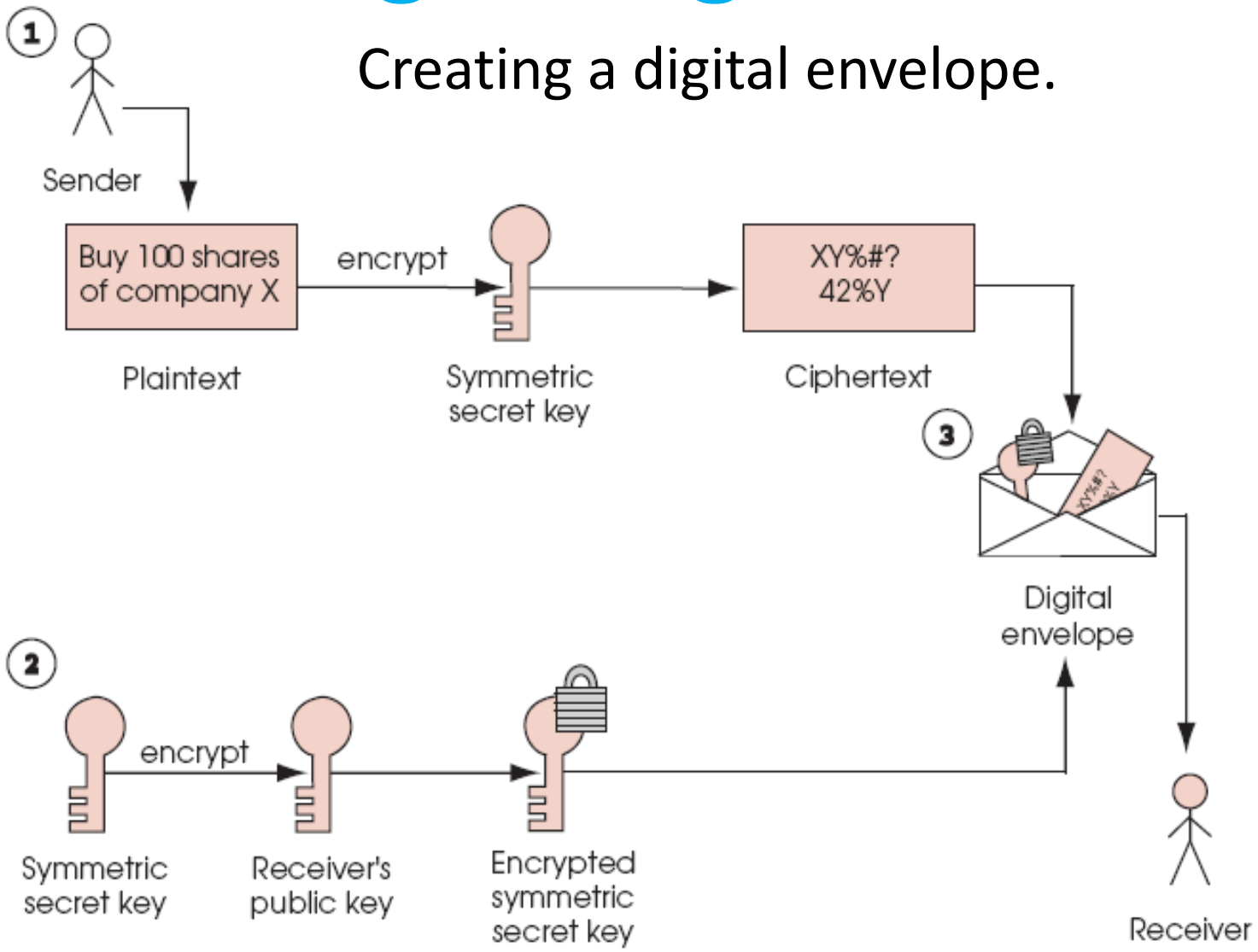
Creating a digital envelope.



Source: E-Business and e-commerce for managers, H. M. Deitel, P. J. Deitel, K. Steinbuhler, Prentice Hall, 2011

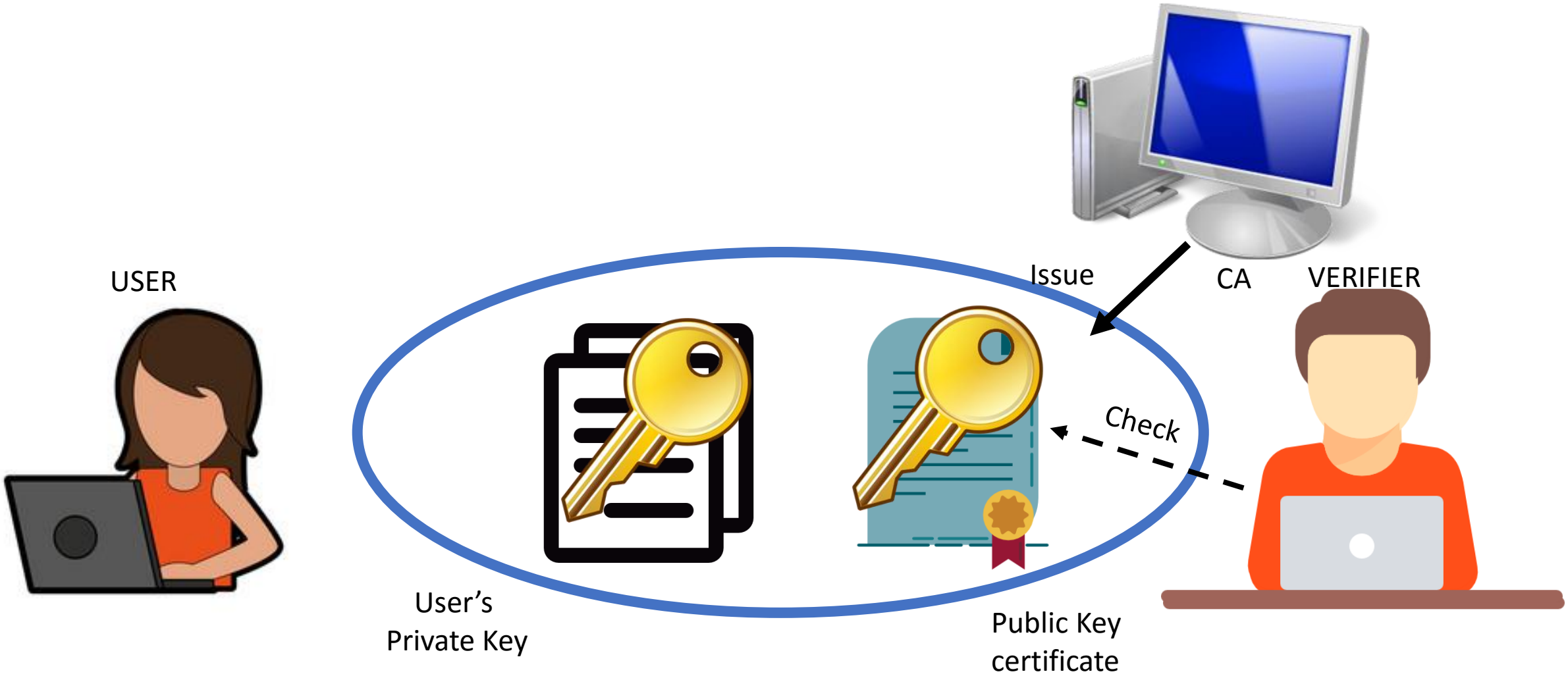
Digital Signatures

Creating a digital envelope.



Source: E-Business and e-commerce for managers, H. M. Deitel, P. J. Deitel, K. Steinbuhler, Prentice Hall, 2011

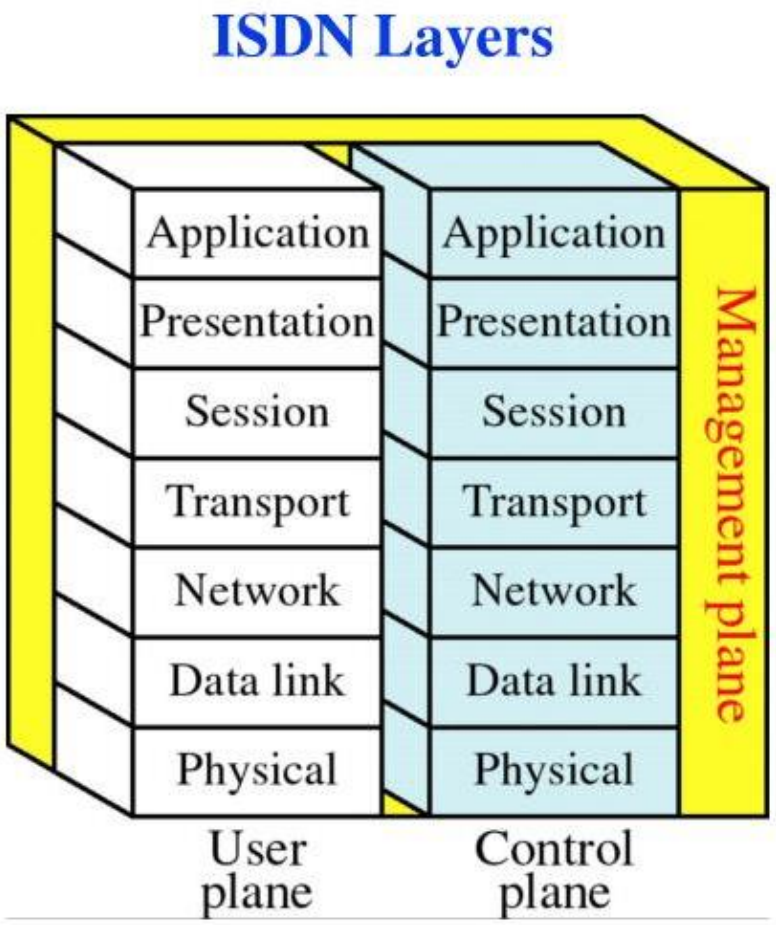
Public-key Infrastructure, Certificates and Certification Authorities



Cryptanalysis

Security Protocols

Secure Sockets Layer (SSL)

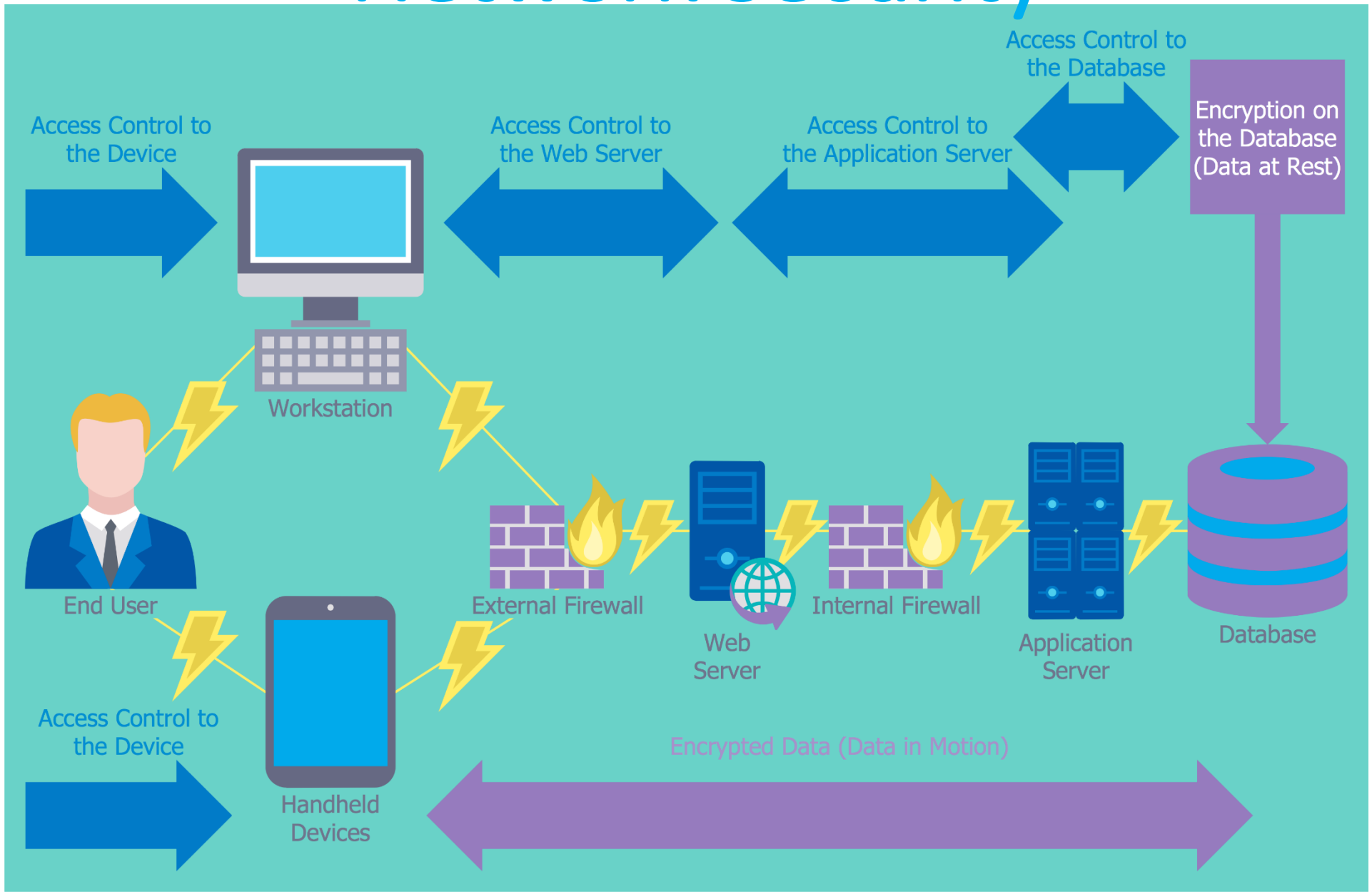


Secure Electronic Transaction

Security Attacks

Viruses
Worms
Trojan horse virus

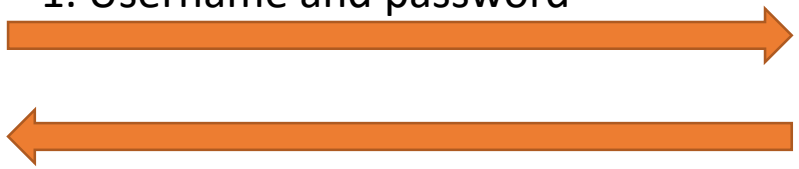
Network Security



Source: http://www.conceptdraw.com/How-To-Guide/network-security-devices

Kerberos

1. Username and password



4. TGT

LOGGED ON!

It checks out un the KDC

Authenti-Cation Service

3. Yes

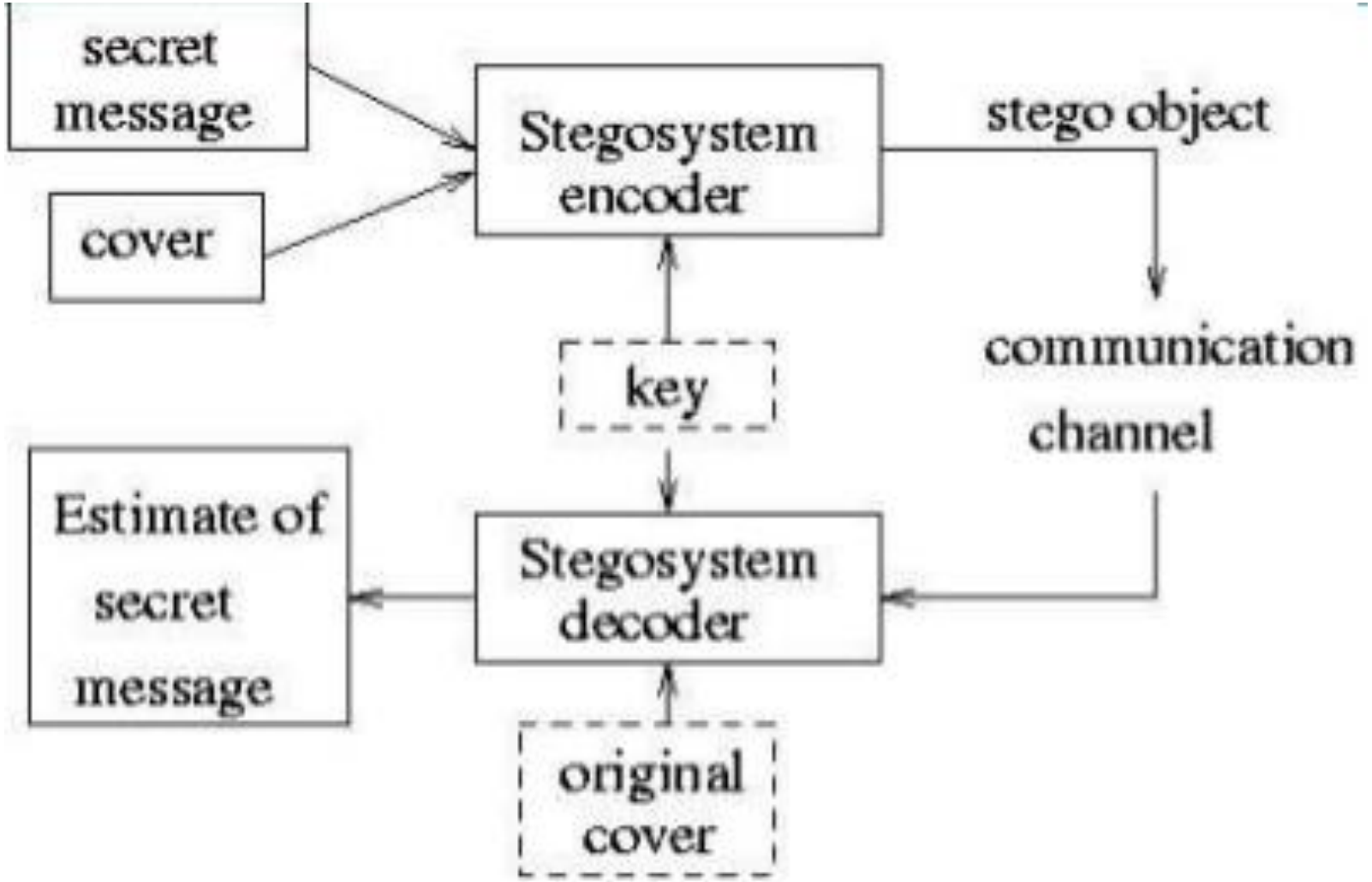
2. Is user/pwd valid?

KDC system

Biometrics


Personal Data
Name
Home Address
Business Address
Identity Card No
Passport No
Driving License
Income Tax No
Car Registration
Confidential Data

Steganography



Next Lecture: Legal and Ethical Issues;
Internet Taxation

Thank you!

My email: d.rasulev1958@gmail.com