original!

Tentamen Nätverkssäkerhet DAVC23

40p + 20p lab = 60p

Hjälpmedel: inga

4 juni 2007 8:15 – 13:15

Ansvarig lärare	Rum	Ankn.	Poäng	Betyg
Thijs Holleboom	5A411	1148	40–46	3
Hans Hedbom	5A433	1157	47–53	4
Simone Fischer-Hübner	5A435	1723	54–60	5

1 Terminology (3p)

Explain the meaning of the following

a. Differential Cryptanalysis

b. Traffic Analysis

c. Key Distribution Problem (when using symmetric encryption).

d. Block Cipher

e. Nonce

f. Pseudo Random Number

2 IPsec (2p)

a. (1p) Describe the two modes in IPsec and show with the help of a figure which headers are added for the Authentication Header Service to the original IP packets, both in transport and in tunnel mode.

b. (1p) Describe how the anti-replay service in IPsec works.

3 SSL/TLS (2p)

a. (2p) Describe the SSL protocol stack. Briefly describe the protocols that are added by SSL and illustrate the location of these protocols in the TCP/IP protocol stack with a figure.

4 Public Key Cryptography and RSA (3p)

a. (2p) What are the principal elements in a public-key cryptosystem?

b. (1p) RSA makes extensively use of modular exponentiation which is a computation intensive process. How can this be done efficiently by examining the individual bits in the exponent? State the algorithm.

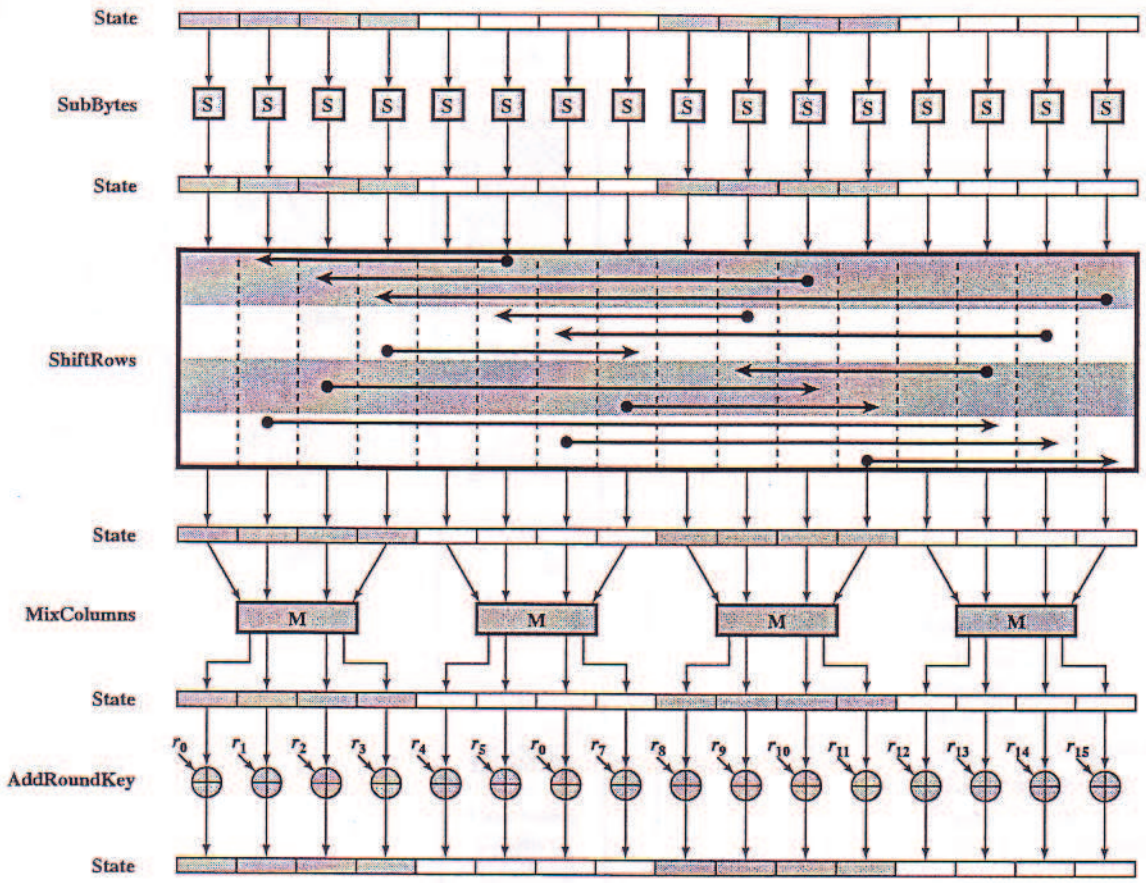

Figure 5.3 AES Encryption Round

5 AES (5p)

Figure 5.3 above shows one round of encryption in the AES algorithm. The figure is taken from Stallings, *Cryptography and network security.*

a. (1p) Describe the *overall structure* of the AES cipher with the help of a figure. (Encryption, Decryption, number of rounds, key expansion, etc.)

b. (2p) Describe in detail the four different stages in one round of encryption with the help of the above figure.

c. (1p) Explain how the decryption process of standard AES can be made equivalent to the encryption process. Refer to the above figure.

d. (1p) Why is 3DES not suitable as a long term replacement of DES?

6 Signatures and Transactions: SET (5p)

SET (Secure Electronic Transaction) is a specification designed to protect credit card transactions on the internet.

a. (1p) Describe the main parties involved in a SET-based transaction, use a figure.

Central in SET based transactions is the Purchase Request, shown in figure 17.10 below.

b. (2p) Describe in detail the contents and purpose of the Dual Signature contained in the Purchase Request.

c. (2p) Describe the function and use of the components shown in the Purchase Request and which security aspects are covered by individual items and operations shown.

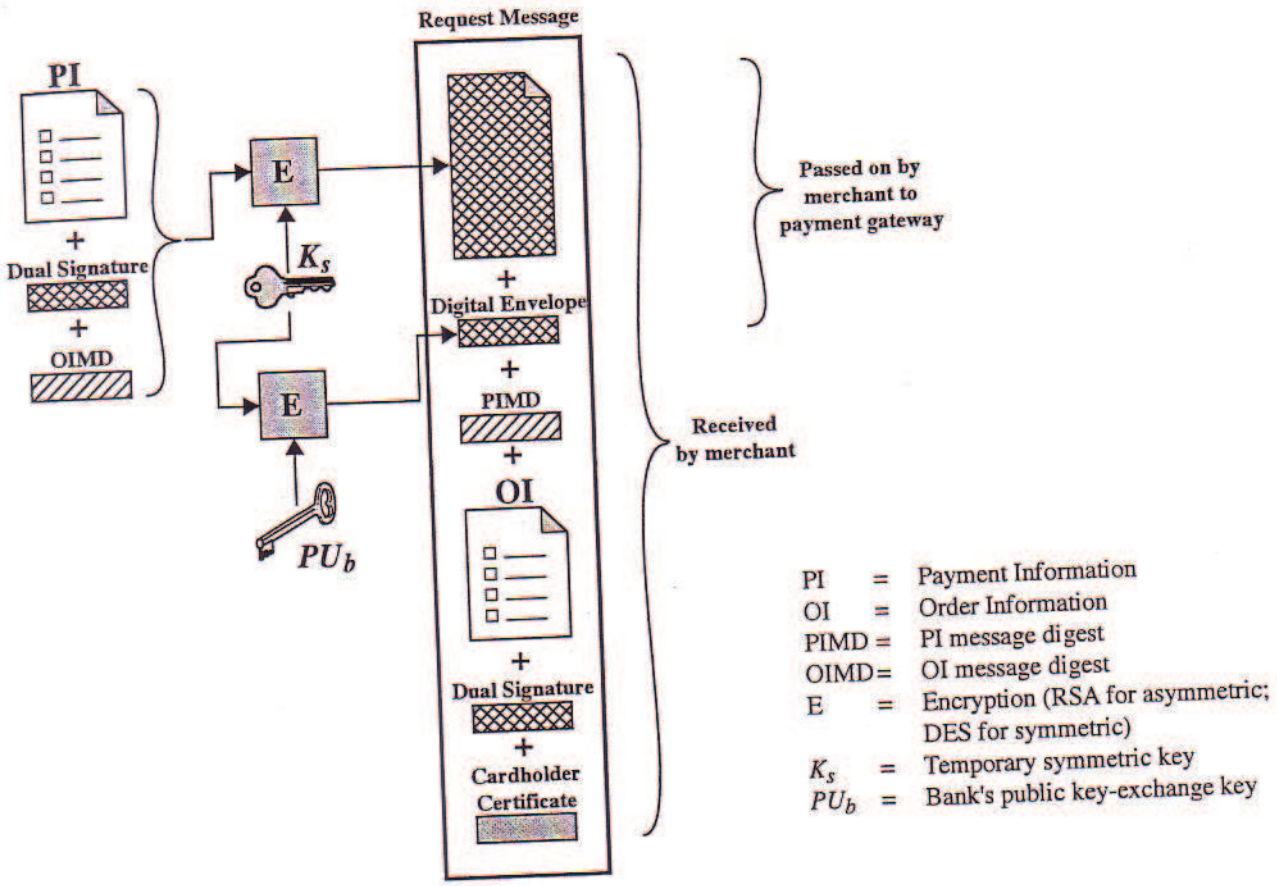

Figure 17.10 Cardholder Sends Purchase Request

7 Kerberos and Vulnerability Analysis (10p)

Besvara denna uppgift på ett separat papper!

1. Kerberos (6p)
   a. (3p) Describe and explain how the kerberos system works.
   b. (1p) What is a realm in the kerberos context. Why is it needed and how is it used?
   c. (2p) The passwords in kerberos are never sent over the network. Despite this the protocol is still vulnerable to password attacks. Explain why this is the case and how it can be attacked (2p).
2. Vulnerability analysis (4p)
   a. (2p) What is vulnerability analysis? Why do we do it and how is it done?
   b. (2p) Explain what an attack-tree is, how it can be used, and how it is constructed.

8 Anonymous communication and Blind Signatures (10p)

Besvara denna uppgift på ett separat papper!

1. Anonymous communication (7p)
   a. (4p) Compare the functionalities of Crowds and Mixnets in providing anonymity.
   b. (1p) With what probability can a web server assume that a Crowd member is the actual sender of a message?
   c. (2p) What is a DC-net and why can it provide perfect sender anonymity?
2. Blind signatures (3p)
   a. (3p) Explain how blind signatures can be used to implement anonymous Ecash (explain the principle –you do not have to describe the exact crypto protocols).