Solutions Final Exam EE/CS 578
Fall 2000

(1) The AH provides integrity and sender authentication for the IP packets. The header is computed by hashing the payload (IP packet) together w/ the secret key

The ESP protocol provides privacy by encrypting of the payload. The payload is either the entire IP packet (tunnel mode) or the upper layer protocol data (transport mode)

(2) $273 = 7 \cdot 39 = 3 \cdot 7 \cdot 13$

$\phi(273) = (3-1)(7-1)(13-1) = 2 \cdot 6 \cdot 12 = 12^2 = 144$

(BTW, twelve dozens $=144$ are a "gross" which is an old measure — this has nothing to do w/ this problem)

Key space $=$ (# poss. "a") $\times$ (# poss. "b")

$= 144 \times 273 = 39312$

(3) Rijndael applies 4 transformation to the data in the 1st round:

α) ByteSub
β) ShiftRow
γ) Mixcolumn
δ) AddRoundKey

α) <u>Byte Sub:</u>

Same S-Box operation is applied to every byte.

There are 16 bytes w/ value $FF_h = 1111\ 1111_2$

<u>1-step</u>: inverse of ~~Aw~~ $x^7+x^6+x^5+x^4+x^3+x^2+x+1$ in $GF(2^8)$

$P(x) = x^8+x^4+x^3+x+1$

ext. EA

(I) $P(x) = [x+1](x^7+x^6+x^5+x^4+x^3+x^2+x+1) + [x^4+x^3+x]$, via long division

$t_2(x) = t_0 - q_1 t_1 = 0 - q_1 = -(x+1) = x+1$

(II) $A(x) = [x^3+x+1]\ (x^4+x^3+x) + [1]$ via long division

$t_3(x) = t_1 - q_2 t_2 = 1 - [x^3+x+1](x+1) = (x^4+x^2+x)+(x^3+x+1)+1$
$= x^4+x^3+x^2$

(III) $x^4+x^3+x = [x^4+x^3+x]\,1 + [0]$

$\Rightarrow A^{-1}(x) = x^4+x^3+x^2 \mod P(x)$

(3) continued

Each column of the new state is computed as

$$\begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{bmatrix} \begin{bmatrix} B(x) \\ B(x) \\ B(x) \\ B(x) \end{bmatrix}$$

$$C_0 = (x + (x+1) + 1 + 1) \cdot B(x) = B(x)$$

$$C_1 = (1 + x + (x+1) + 1)\ B(x) = B(x)$$

$$C_2 = \qquad = B(x)$$

$$C_3 = \qquad B(x)$$

=> state after MixColumn still consists of 16 Bytes w/ value $B = 16_h$

8.) Add Round Key

Since subkey is all-one, all bits are flipped

$$B \oplus (1111\ 1111) = 1110\ 1001_2 = E9$$

=> output after final round

$$\underbrace{E9 \quad E9 \quad E9 \ \ldots \ E9}_{16 \text{ times}}$$

③ continued

2. Step: Mult. of $A^{-1}(x)$ by matrix + vector add.

$A = 0001\ 1100$

$B := ByteSub(A) =$

$$B = M \cdot A + V = \begin{bmatrix}1\\0\\1\\0\\1\\1\\1\\0\end{bmatrix} + \begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{bmatrix} = \begin{bmatrix}0\\1\\1\\0\\1\\0\\0\\0\end{bmatrix}$$

$B = 16_h = (0001\ 0110) \Longleftrightarrow B(x) = x^4 + x^2 + x$

$\Rightarrow$ State consists of 16 (=128/8) identical Bytes:

$16,\ 16,\ 16\ \cdots\ 16_h$

β) ShiftRow transformation does not change data, since it's only a byte re-ordering.

γ) Mixcolumn

performs mult. of $B(x)$ w/ $1, x,$ and $x+1$

$1 \quad B(x) = x^4 + x^2 + x = 0001\ 0110$ [not needed]

$x \quad B(x) = x^5 + x^3 + x^2 = 0010\ 1100$

$(x+1)\ B(x) = (x^5+x^3+x^2) + (x^4+x^2+x) = x^5 + x^4 + x^3 + x = 00111010$

(4) $x = y^a \bmod n$

$a = b^{-1} \bmod \phi(n)$

$\phi(n) = 100 \cdot 106 = 10\,600$; $n = 10\,807$

extended EA: w/ $\phi(n)$, b

$10600 = 2 \cdot 4497 + 1606$; $t_2 = t_0 - q_1 t_1 = -q_1 = -2$

$4497 = 2 \cdot 1606 + 1285$; $t_3 = t_1 - q_2 t_2 = 1 - 2(-2) = 5$

$1606 = 1 \cdot 1285 + 321$; $t_4 = t_2 - q_3 t_3 = -2 - 1(5) = -7$

$1285 = 4 \cdot 321 + 1$; $t_5 = t_3 - q_4 t_4 = 5 - 4(-7) = 33$

$321 = 321 \cdot 1 + 0$

$a = 33 \equiv 4497^{-1} \bmod 10\,600$

[check $33 \cdot 4497 = 148\,401 \equiv 1 \bmod 10600$]

$7411^{33} = 7411^{100001}$

$7411^2 \equiv 1747 \bmod n$

$7411^4 = 7411^{100} \equiv 4435 \bmod n$

$7411^8 = 7411^{1000} \equiv 485 \bmod n$

$7411^{16} = 7411^{10000} \equiv 8278 \bmod n$

$7411^{32} = 7411^{100000} \equiv 8904 \bmod n$

$7411^{33} = 8904 \cdot 7411 \equiv \underline{2 \bmod n}$

5 a) $|\mathbb{Z}_{131}^*| = 130 = 13 \cdot 10 = 2 \cdot 5 \cdot 13$

poss. orders $= \{1, 2, 5, 10, 13, 26, 65, 130\}$

check 2: $70^2 = 53 \mod p \Rightarrow \operatorname{ord}(70) \neq 2$

check 5: $70^5 = 70^2 \cdot 70^2 \cdot 70 = 130 \mod p \Rightarrow \operatorname{ord}(70) \neq 5$

check 10: $70^{10} = (70^5)^2 = 130^2 \equiv 1 \mod p \Rightarrow \underline{\underline{\operatorname{ord}(70) = 10}}$

b) $\alpha^{774} \equiv \alpha^{774 \mod 10} \equiv \alpha^4 \mod 131$

$70^4 = (70^2)^2 = 53^2 \equiv \underline{\underline{58 \mod 131}}$

6 a)

1) decryption of y using symmetric alg. w/ key K_1

$$d_{K_1}(y) = x \| H(K_2 \| x)$$

2) concatenate K_2 and x, where K_2 is the 2nd secret key of the receiver

3) compute hash of $K_2 \| x$

4) compare computed hash value with the one received by decryption in 1)

b)

1.) decrypt as in 1a)

$$d_K(y) = x \| sig(H(x))$$

2) feed h(x) and sig(H(x)) into verification algorithm and check whether signature is valid: Ver. alg. needs public key of sender

(7)

Protocol A

1) Confidendiality – yes, given through encryption

2) Integrity – yes, data manipulation (by Oscar) will result in a corrupted y value, which will most likely not lead to a valid pair $\tilde{x}$, $\tilde{H}(K_2 \| \tilde{x})$

3) Non-repudiation – NO, both Alice and Bob can generate valid message.

$$y_{K_1}(x \| H(K_2 \| x))$$

A neutral 3rd party can not decide who generated the message

Protocol D

1) Confidentiality – yes, as above

2) Integrity – yes, manipulation of y will most likely result in a pair

$$(\tilde{X}, \widetilde{sig}_{K_{pr}}(\ ))$$

For which the verification will not check out

3) Non-repudiation – yes, only sender can generate messages w/ valid signatures