CIS 3362 10/12/26

1) AES Key Schedule

2) AES Code - look @

3) Symm Cipher Modes

4) WED IS EXAM #2 !!!

FILLED

UNFILLED

type 32 bits (8 HEX) (4 bytes)

```
KeyExp(byte key[16], word w[44]) {
```

RO key be key // for (i=0; i<4; i++)

is sent

w[i] = (key[4i], key[4i+1], key[4i+2], key[4i+3])

Concat these 4 bytes

```
w temp
for (i=4; i<44; i++) {

    temp = w[i-1]
    if (i%4 == 0)
        temp = SubWord(RotWord(temp)) ⊕ (Rcon[i/4], 00,00,00)
    w[i] = w[i-4] ⊕ temp
```

→ ROTWORD cyclic left shift by 1 byte

SUBWORD IS USING S-BOXES

What's pattern w/ RCON

1 0000 0001
2 0000 0010
3 0000 0100
4 0000 1000
5 0001 0000
6 0010 0000
7 0100 0000
8 1000 0000
9 0001 1011 — IS $x^9 \bmod x^8+x^4+x^3+x+1$
10 0011 0110 — IS $x^{10} \bmod x^8+x^4+x^3+x+1$

TRACE THROUGH

	w[35]	ROTWORD	SUBWORD
w[36]	7F8D292E (hex)	8D292F7F	5DA515D2

RCON[1/4]	Alg XOR w/ RCON	w[32]
1B000000	46A515D2	EAD27321
5DA515D2		

w[36] = 46A515D2
⊕ EAD27321
AC7766F3

1101
1110
1010
110
1100

$a \times b$ algorithm in code

$(x^5 + x^2 + 1) \times b$

$= b + x^2 b + x^5 b$

in code, I iteratively compute

$b, bx, bx^2, bx^3, \ldots$

pow2

just add terms when bit corresponding is ON in a.

Symmetric CIPHER Modes

symmetric cryptography algorithms specify how to encrypt 1 block.

OUR FULL DOCUMENT MIGHT BE

$P_1 P_2 P_3 P_4 \ldots P_n$ n blocks (128 bits/blocks)

EASIEST: Electronic Codebook

for $i = 1$ to n

$C_i = E(K, P_i)$

encrypt each block separately w/ the same key!

#2 Cipher Block Chaining

$C_0 = IV$ (initialization vector)
for $i = 1$ to n
$C_i = E(K, C_{i-1} \oplus P_i)$

What's being encrypted ISN'T plaintext blocks

Can not parallelize this

3 Output Feedback Mode

~~#4 Cipher Feedback Mode~~

$K_0 = IV$
for $i = 1$ to n:
$K_i = E(K, K_{i-1})$
$C_i = P_i \oplus K_i$

// Can't do in parallel except that... K_i's could be precomputed!

#3) ~~Output Feedback Mode~~

~~$K_0 = IV$~~

#4) Cipher Feedback Mode

$C_0 = IV$
for $i = 1$ to n
$K_i = E(K, C_{i-1})$
$C_i = P_i \oplus K_i$

// Can't parallelize

#5 Counter Mode

Counter array that stores pre-chosen values could be 1, 2, 3, ...

for $i = 1$ to n

$$K_i = E(K, \text{counter}[i])$$

$$C_i = P_i \oplus K_i$$