

## ECE 297:11 Lecture 5

### 64-bit Secret-Key Ciphers: IDEA & RC5

---

---

---

---

---

---

---

---

**IDEA** *X. Lai, J. Massey  
ETH, 1990-91*

- 128-bit key (**billion machines** each checking **billion keys per second** still would require **10 trillion years**, to check all keys)
- used in **PGP** (Pretty Good Privacy) - the most popular public domain program for secure e-mail
- constructed to provide an absolute resistance against **differential cryptanalysis**

---

---

---

---

---

---

---

---

### IDEA

Three basic operations:

$X$	$X$	$X$
$Y = X \oplus K$	$Y = X + K \pmod{2^{16}}$	$Y = X \cdot K \pmod{(2^{16}+1)}$

where 0 represents  $2^{16}$

Corresponding inverse operations:

$Y$	$Y$	$Y$
$X = Y \oplus K$	$X = Y + (-K) \pmod{2^{16}}$	$X = Y \cdot K^{-1} \pmod{(2^{16}+1)}$

---

---

---

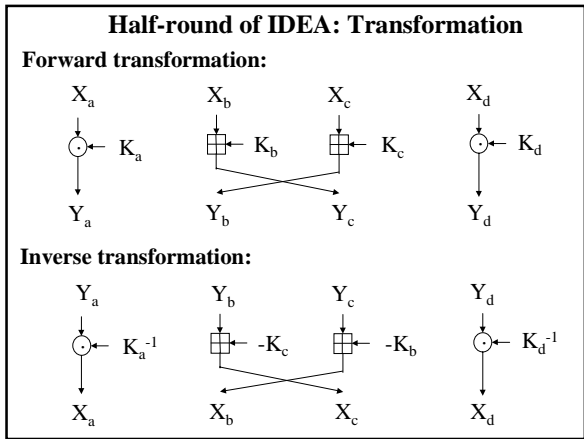
---

---

---

---

---




---

---

---

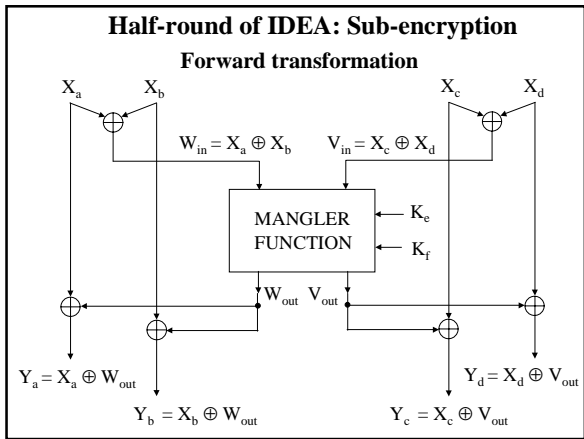
---

---

---

---

---




---

---

---

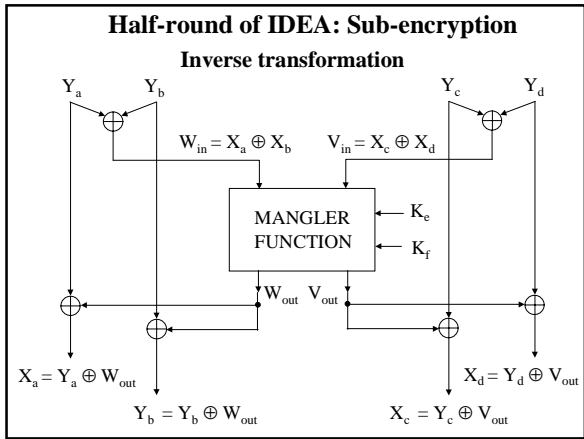
---

---

---

---

---




---

---

---

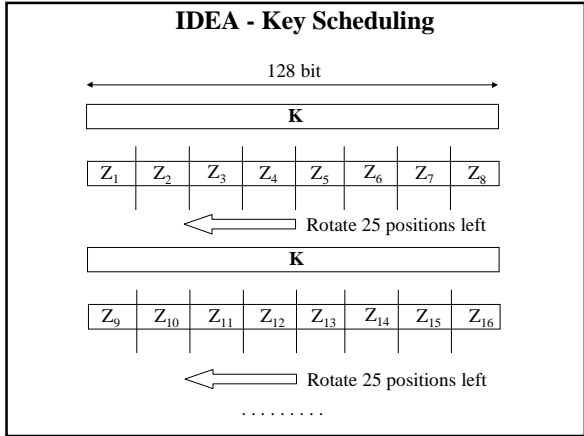
---

---

---

---

---




---

---

---

---

---

---

---

---

**Implementing IDEA in Hardware**

---

---

---

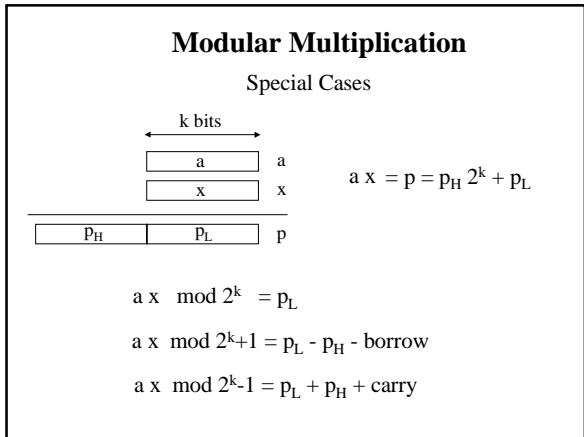
---

---

---

---

---




---

---

---

---

---

---

---

---

### Modular Multiplication

Special Case (1)

$$\begin{aligned} a \times \text{mod } 2^{k+1} &= (p_H 2^k + p_L) \text{mod } (2^{k+1}) = \\ &= (p_H(2^{k+1}-1) + p_L) \text{mod } (2^{k+1}) = \\ &= p_L - p_H \text{mod } (2^{k+1}) = \\ &= \begin{cases} p_L - p_H & \text{if } p_L - p_H \geq 0 \\ p_L - p_H + (2^{k+1}) & \text{if } p_L - p_H < 0 \end{cases} \\ &= p_L - p_H + \text{borrow} \end{aligned}$$

borrow = borrow from subtraction  $p_L - p_H$

---

---

---

---

---

---

---

---

### Modular Multiplication

Special Case (2)

$$\begin{aligned} a \times \text{mod } 2^{k-1} &= (p_H 2^k + p_L) \text{mod } (2^{k-1}) = \\ &= (p_H(2^k \text{mod } 2^{k-1}) + p_L) \text{mod } (2^{k-1}) = \\ &= p_H + p_L \text{mod } (2^{k-1}) = \\ &= \begin{cases} p_H + p_L & \text{if } p_H + p_L < 2^{k-1} \\ p_H + p_L - (2^{k-1}) & \text{if } p_H + p_L \geq 2^{k-1} \end{cases} \\ &= p_L + p_H + \text{carry} \end{aligned}$$

carry = carry from addition  $p_L + p_H$

---

---

---

---

---

---

---

---

**RC5**

---

---

---

---

---

---

---

---

**RC5** *Ron Rivest, MIT, 1994*

(Ron's Code 5, Rivest's Cipher 5)

- **variable key length** (40 bits in the former export version, 128 bits to achieve the same strength as IDEA)
- **variable block size** (depends on the processor word length)
- **variable number of rounds** (determines resistance to linear and differential cryptanalysis; for 9 rounds this resistance is greater than for DES)
- **simplicity of description**

---

---

---

---

---

---

---

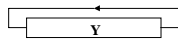
---

**RC5**

**One of the fastest ciphers**

Basic operation

Rotation by a variable number of bits



$$Y = Y \ll X$$

---

---

---

---

---

---

---

---

**RC5 w/r/b**

**w - word size in bits**  $w = 16, 32, 64$

input/output block = 2 words =  $2 \cdot w$  bits

Typical value:

$w=32 \Rightarrow$  64-bit input/output block

**r - number of rounds**

**b - key size in bytes**  $0 \leq b \leq 255$

key size in bits =  $8 \cdot b$  bits

**Recommended version: RC5 32/12/16**

**64 bit block**

**12 rounds**

**128 bit key**

---

---

---

---

---

---

---

---

<b>RC5</b>	
<b>Encryption</b>	<b>Decryption</b>
$A \parallel B = M$  $A = A + S[0]$ $B = B + S[1]$  for $i = 1$ to $r$ do { $A = (A \oplus B) \lll B + S[2i]$ $B = (B \oplus A) \lll A + S[2i+1]$ }  $C = A \parallel B$	$A \parallel B = C$  for $i = r$ downto $1$ do { $B = ((B - S[2i+1]) \ggg A) \oplus A$ $A = ((A - S[2i]) \ggg B) \oplus B$ }  $B = B - S[1]$ $A = A - S[0]$  $M = A \parallel B$

---

---

---

---

---

---

---

---

**RC5 - Key Scheduling**

$k$  bits of the main key

↓

$2 \cdot r + 2$  round keys =  $(2 \cdot r + 2) \cdot w$  bits

Two magic constants:

$P_w = \text{Odd}((e-2) \cdot 2^w)$        $e$  - base of natural logarithms  
 $e = 2.7182\dots$

$Q_w = \text{Odd}((\phi-1) \cdot 2^w)$        $\phi$  - golden ratio =  $\frac{x}{y} = \frac{y}{x-y} = 1.6180\dots$

---

---

---

---

---

---

---

---

**RC5 - Key Scheduling**

**Initialize**

$S[0] = P_w$   
 for  $i = 0$  to  $t-1$  do  
 $S[i] = S[i] + Q_w$

**Mix**

$i = j = 0$   
 $A = B = 0$   
 do  $3 \cdot \max\{t, c\}$  times  
 {  
 $A = S[i] = (S[i] + A + B) \lll 3$   
 $B = L[j] = (L[j] + A + B) \lll (A+B)$   
 $i = (i+1) \bmod t$   
 $j = (j+1) \bmod c$   
 }

$t = 2 \cdot r + 2$   
  
 $c = \left\lceil \frac{8 \cdot b}{w} \right\rceil$

---

---

---

---

---

---

---

---

<b>RC5 - Resistance to differential and linear cryptanalysis</b>							
<b>Plaintext requirement</b>							
<b># rounds</b>	4	5	6	7	9	12	13
<b>Differential Cryptanalysis</b>	$2^{22}$	$2^{26}$	$2^{32}$	$2^{37}$	<b><math>2^{46}</math></b>	$2^{63}$	$>2^{64}$
<b>Linear Cryptanalysis</b>	$2^{37}$	<b><math>2^{47}</math></b>	$2^{57}$	$>2^{64}$			

Differential cryptanalysis cannot be applied to RC5 with #rounds  $\geq 13$   
 Linear cryptanalysis cannot be applied to RC5 with #rounds  $\geq 7$

---

---

---

---

---

---

---

---

## Security of Modern Ciphers

---

---

---

---

---

---

---

---

<b>Resistance of modern ciphers against known attacks</b>	
Proprietary ciphers built in application software	mostly insecure, seconds on PC
Proprietary ciphers with unknown specification	uncertain, impossible to verify
40-bit "international" version of ciphers	Keys recoverable using several hours with a small network of computers
DES	Keys can be recovered within 24 hours using a specialized machine worth about \$300,000
Triple DES, DESX, RC5, IDEA	<b>All known attacks impractical</b>

---

---

---

---

---

---

---

---

**State of research regarding the security of  
secret-key ciphers**

- limited number (20-50) of researchers actively involved in cryptanalysis and design of new ciphers
- number of published ciphers > 50
- evaluations of the cipher strength given by designers typically unreliable

**“Honest” cipher = the best known attack  
is an exhaustive key search attack**

**One can rely only on ciphers analyzed by a large group  
of qualified researchers**

---

---

---

---

---

---

---

---