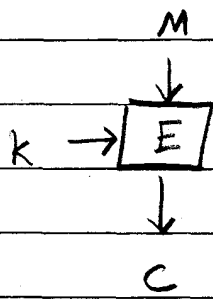


Block Ciphers

09/2.



keys
 $E: \{0,1\}^L \times \{0,1\}^l \rightarrow \{0,1\}^L$

$E(k, \cdot)$ and $E^{-1}(k, \cdot)$ are easy to compute and are permutations

Ex. keys = $n \times n$ invertable matrices over \mathbb{F}_2 ,
 $C = M = n$ -vectors over \mathbb{F}_2

$E(k, m) = k \cdot m$

$E^{-1}(k, m) = k^{-1} \cdot m$

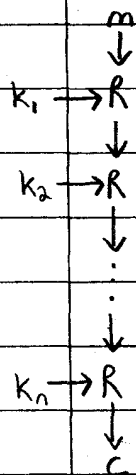
If attacker can obtain $(m_1, c_1), (m_2, c_2), \dots, (m_n, c_n)$ then he can solve system of n linear equations to get

Ex. $R(k_i, x) = \frac{1}{x+k_i}$

every element has an inverse, no two map to the same \Rightarrow permutation

$k_i, x \in \mathbb{F}_{2^{128}} \quad \frac{1}{0} = 0$

$E(k_1 || k_2 || \dots || k_n, m) = R(k_n, R(k_{n-1}, \dots, R(k_1, m) \dots))$



$R(k_2, R(k_1, x)) = \frac{1}{R(k_1, x) + k_2}$

$= \frac{1}{\frac{1}{x+k_1} + k_2} = \frac{x+k_1}{x+k_1 + k_2}$

$= \frac{x+k_1}{1 + k_2x + k_1k_2}$

$= \frac{x+k_1}{k_2x + (k_1k_2+1)}$

each round of R looks like \rightarrow

$\frac{ax+b}{cx+d}$

two equations of this form multiplied \Rightarrow another equation of this form

$$f_{a,b,c,d}(x) = \frac{ax+b}{cx+d}$$

$$f_{a_2,b_2,c_2,d_2} \circ f_{a_1,b_1,c_1,d_1}(x)$$

f_2

f_1

$$= \frac{a_2 f_1(x) + b_2}{c_2 f_1(x) + d_2}$$

$$= \frac{a_2 \frac{a_1 x + b_1}{c_1 x + d_1} + b_2}{c_2 \frac{a_1 x + b_1}{c_1 x + d_1} + d_2}$$

$$= \frac{a_2 a_1 x + a_2 b_1 + b_2 c_1 x + b_2 d_1}{c_2 a_1 x + c_2 b_1 + d_2 c_1 x + d_2 d_1}$$

$$= \frac{a_2 a_1 x + a_2 b_1 + b_2 c_1 x + b_2 d_1}{(a_1 c_2 + c_1 d_2)x + (b_1 c_2 + d_1 d_2)}$$

$$= \frac{(a_2 a_1 + b_2 c_1)x + (a_2 b_1 + b_2 d_1)}{(a_1 c_2 + c_1 d_2)x + (b_1 c_2 + d_1 d_2)}$$

$$= \frac{(a_2 a_1 + b_2 c_1)x + (a_2 b_1 + b_2 d_1)}{(a_1 c_2 + c_1 d_2)x + (b_1 c_2 + d_1 d_2)}$$

$$= \frac{(a_2 a_1 + b_2 c_1)x + (a_2 b_1 + b_2 d_1)}{(a_1 c_2 + c_1 d_2)x + (b_1 c_2 + d_1 d_2)}$$

$$= \frac{(a_2 a_1 + b_2 c_1)x + (a_2 b_1 + b_2 d_1)}{(a_1 c_2 + c_1 d_2)x + (b_1 c_2 + d_1 d_2)}$$

$$E(k, x) = \frac{ax+b}{cx+d} \text{ for some } a, b, c, d$$

\Rightarrow need 4 plaintext/ciphertext pairs

$$\frac{am_1 + b}{cm_1 + d} = c_1$$

$$m_1 a + b = (c_1 m_1 + d) c_1$$

AES - Advanced Encryption Standard

$$M = C = \mathbb{F}_2^{16} \approx \{0, 1\}^{128} \text{ (vector of 16 bytes = input)}$$

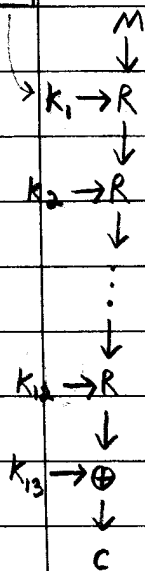
$L =$ a particular 128×128 invertible matrix over \mathbb{F}_2^{128}

$$R(k, x) = L \cdot (x_1 \oplus k_1, x_2 \oplus k_2, \dots, x_{16} \oplus k_{16}) \quad \frac{1}{0} = 0$$

$$k = k_1 \parallel k_2 \parallel \dots \parallel k_{16}$$

$K \rightarrow \boxed{G}$

each k is a 128-bit vector



Conj. AES is a $(t, q, \frac{t}{2^{128}} + \frac{q}{2^{128}})$ PRF

Defn. E is a (t, q, ϵ) Pseudo-Random Permutation (PRP) if $\forall A$ running in time t and making at most q oracle queries,

$$\text{Adv}_A = |\Pr[A^E = 1; k \leftarrow U] - \Pr[A^{\Pi} = 1; \Pi \leftarrow \text{Perms}]| \leq \epsilon$$

$$E[\# \text{ of pairs w/ same birthday}] = \frac{253}{365} \approx \frac{2}{3}$$

$\{0, 1\}^{128}$	query	answer
\downarrow	x_1	y_1
$\boxed{\oplus}$	x_2	y_2
\downarrow	\vdots	\vdots
$\{0, 1\}^{128}$	x_q	y_q

Is \oplus a permutation?

If you ever see $y_i = y_j$, where $x_i \neq x_j$, then \oplus is not a permutation

Strategy ① make q distinct queries.

② if any output is repeated, return 1

③ else return 0

PRP-PRF Switching Lemma

Lemma: Perms $(\Sigma_{0, 13^q})$ is $(\epsilon, q, \frac{q^2}{2^{t+1}})$ indistinguishable from Funcs $(\Sigma_{0, 13^q} \rightarrow \Sigma_{0, 13^q})$

Proof: R/P init:

Table = empty hash table;

bad = false;

query (x)

if $x \in \text{domain}(\text{Table})$

return Table[x];

$y \xleftarrow{\$} U_n$;

if $\in \text{range}(\text{table})$

bad = true;

$y \xleftarrow{\$} \Sigma_{0, 13^q} \setminus \text{range}(\text{Table});$ } $\left. \begin{array}{l} \text{in } P, \\ \text{not } R \end{array} \right\}$

return y;

① R implements a random function

② P implements a random permutation

\Rightarrow At each query, result y is equally likely to be any element of $\Sigma_{0, 13^q} \setminus \text{range}(\text{Table})$

\Rightarrow This generates a permutation at random

③ If after q queries, bad=false, then

$$\Pr[A^R=1] = \Pr[A^P=1]$$

$$\text{Adv } A = |\Pr[A^R=1] - \Pr[A^P=1]|$$

$$= |\Pr[A^R=1 | \text{bad=false}] \Pr[\text{bad=false}] +$$

$$\Pr[A^R=1 | \text{bad=true}] \Pr[\text{bad=true}] - \Pr[A^P=1 | \text{bad=false}] \Pr[\text{bad=false}]$$

$$- \Pr[A^P=1 | \text{bad=true}] \Pr[\text{bad=true}] \leq \Pr[\text{bad=true}]$$