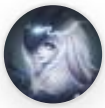


cmhernandezdel
www.wuolah.com/student/cmhernandezdel

algoritmoscripto.pdf

Resumen de algoritmos del curso

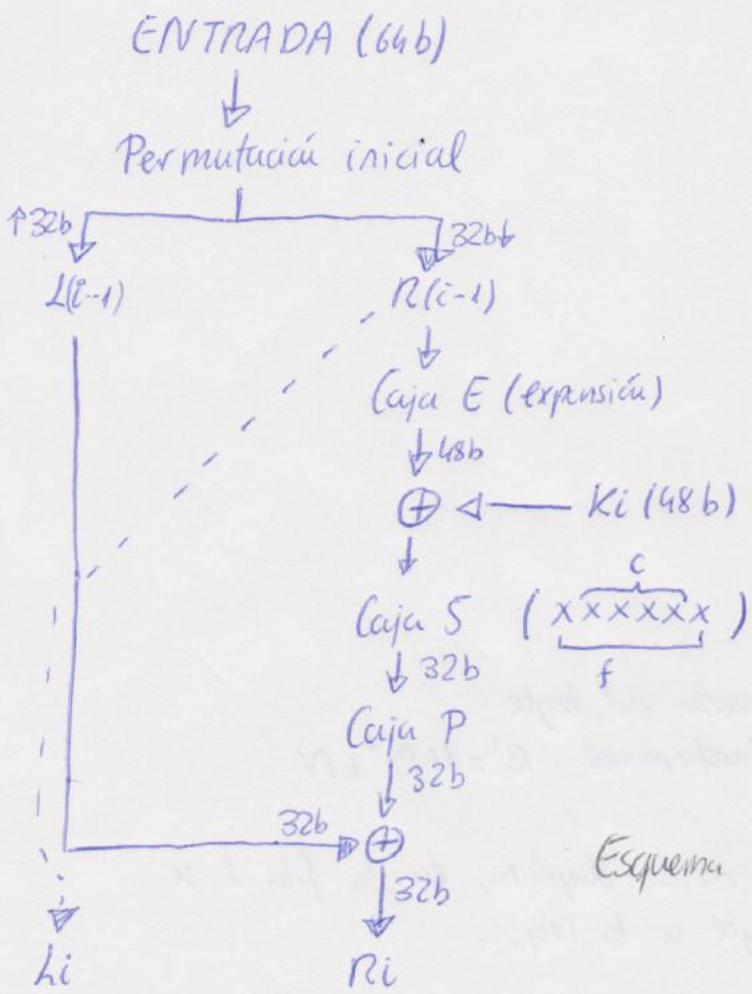
2° Criptografía y Seguridad Informática

Grado en Ingeniería Informática

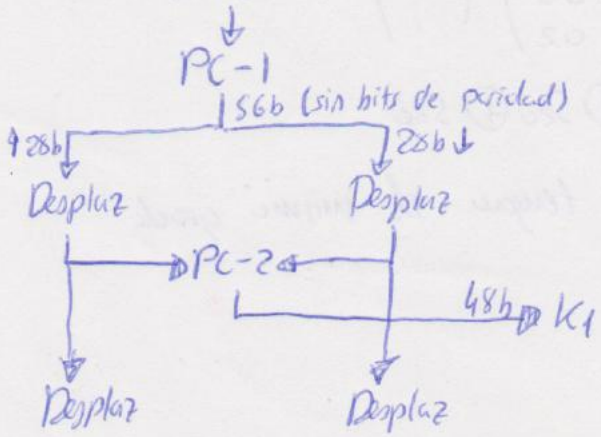
Escuela Politécnica Superior
UC3M - Universidad Carlos III de Madrid

TEMA 4. CIFRADORES SIMÉTRICOS

4.1 Cifrado DES



Esquema del cifrado DES.

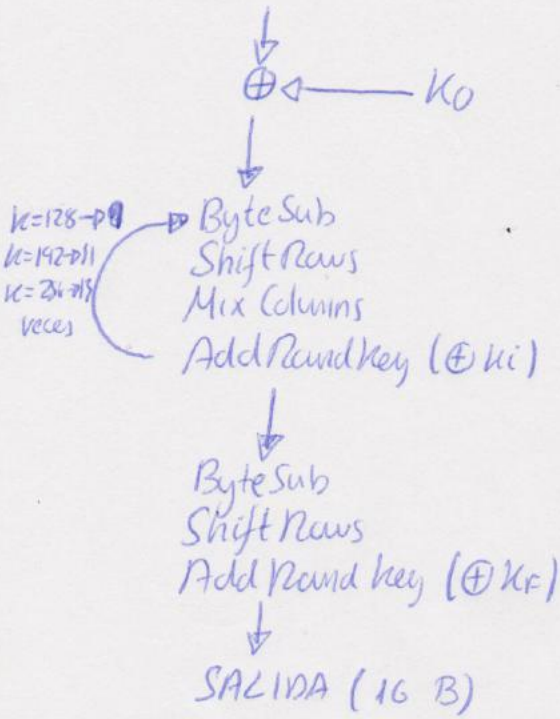


Esquema de obtención de las claves internas

4.2 Cifrado AES

ENTRADA (16 B)

$K = 128, 192$ ó 256 bits
$E = 128$ bits



SALIDA (16 B)

- **ByteSb:** 1) Hallar el inverso del byte
  2) Aplicar la transformación $B' = M \cdot B^{-1} + N$

- **ShiftRows:** En la fila 0 no se desplaza, en la fila 1 se desplaza un byte a la izq...

- **MixColumns:**

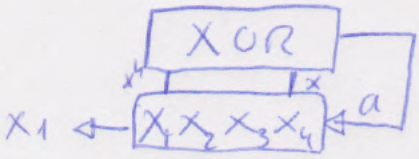
$$\begin{pmatrix} S'_{00} \\ S'_{10} \\ \vdots \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} S_{00} \\ S_{10} \\ \vdots \end{pmatrix}$$

$$S'_{00} = 02 \cdot S_{00} \oplus 03 \cdot S_{10} \oplus S_{20} \oplus S_{30}$$

Para reducir eliminamos los que tengan el mismo grado que el módulo.

4.3 Cifrado LFSR

Nos dan una semilla, $X_1X_2X_3X_4$ y un polinomio (ej. x^4+x+1)



Esto se va aplicando hasta que salga la semilla de nuevo.
Si $p(x)$ es primo, T es máxima (2^n-1).

4.4 Cifrado RC4

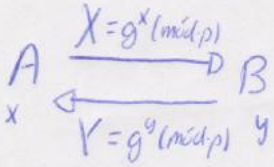
Partimos de un vector S de 256 posiciones.

```
for (i=0; i<256; i++){
    j = j + S[i] + K[i];
    swap (S[i], S[j]);
    {
```

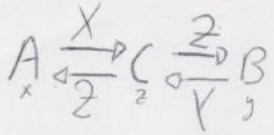
S[0]=0, S[1]=1...

TEMA 6. CIFRADORES ASIMÉTRICOS

6.1 Algoritmo de Diffie-Hellman (negociación de claves)

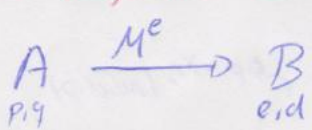


1. A y B eligen un primo p, y un generador g, públicos.
2. A elige x, y envía a B: $X = g^x \pmod p$
3. B elige y, y envía a A: $Y = g^y \pmod p$
4. A calcula Y^x y B X^y, ambos dan el mismo número que será K, la clave.



Man in the middle: K_{AC}, K_{BC} y les pilla los mensajes, no la clave

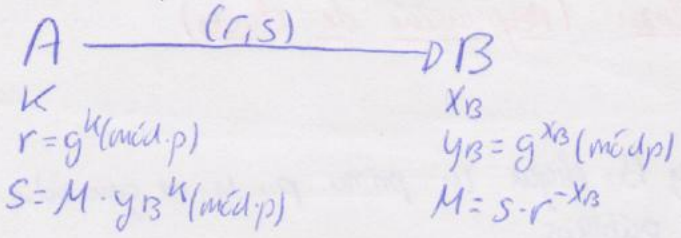
6.2 Algoritmo RSA



1. A elige p y q primos, tal que $n = p \cdot q$ (n es pública, p y q no).
2. B elige e, tal que $\text{mcd}(e, \phi n) = 1$. Esta es su clave pública.
3. A su vez, B calcula $d = e^{-1} \pmod{\phi n}$. Esta es su clave privada.
4. A envía $M^e = C$, el cifrado. $\pmod n$
5. B descifra con $M = C^d \pmod n$

6.3 Algoritmo de El Gamal

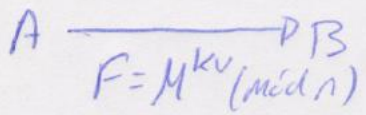
p, g



1. B elige p y g, que son públicos.
2. B elige x_B como clave privada
3. B calcula $y_B = g^{x_B} \pmod p$, como clave pública.
4. A elige k aleatorio tal que $\text{mcd}(k, p-1) = 1$.
5. A calcula $g^k \pmod p = r$.
6. A calcula $s = M \cdot y_B^k \pmod p$
7. A envía $C = (r, s)$.
8. B descifra mediante $M = s \cdot r^{-x_B}$ con $r^{-x_B} = r^{\phi p - x_B} \pmod p$

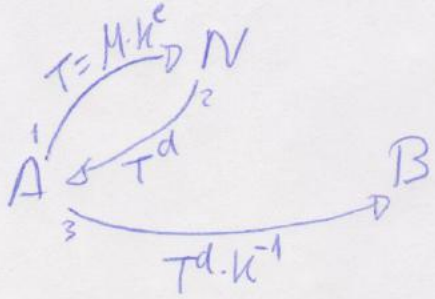
TEMA 7. FIRMA DIGITAL

7.1 Firma RSA



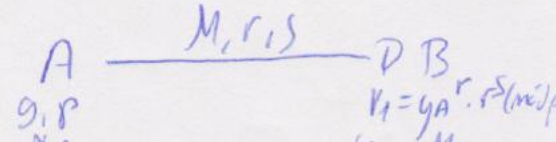
1. A elige p, q primos, $n = pq$
2. A elige k_u, clave pública
3. A calcula $k_v = k_u^{-1}$ (mód. ϕn), privada.
4. A envía $F = M^{kv}$ (mód.n)
5. B valida $M = F^{k_u}$ (mód.n)

7.2 Firma opaca con RSA



1. A envía $T = M \cdot K^e$ al notario, donde K es el factor de encubrimiento y e la clave pública del notario.
2. El notario firma T y envía a A T^d.
3. A calcula $M^d = T^d \cdot K^{-1}$ (mód.n).
4. A envía M^d a B
5. B valida con la clave pública del notario

7.3 Firma El Gamal



1. A elige g y p, públicos.
2. A elige x_A, que es su clave privada
3. A calcula y_A, clave pública, como $y_A = g^{x_A}$ (mód p) y la envía a B.
4. A genera k aleatorio y coprimo a p-1.
5. A calcula $r = g^k$ (mód p)
6. A calcula $s = (M - x_A \cdot r) \cdot k^{-1}$ (mód p-1)
7. A envía M, r, s a B.
8. Para verificar, B calcula $V_1 = y_A^r \cdot r^s$ (mód p) y $V_2 = g^M$ (mód p). Si $V_1 = V_2$, valida.