RSA

$n = pq$

$\phi(n) = (p-1)(q-1)$

Escogemos $e \leq \phi(n)$ coprimo con $\phi(n)$

$K_E = (n, e)$ $\qquad P \xrightarrow{\text{cifrado}} P^e \pmod n$

$d = e^{-1} \pmod{\phi(n)}$

$K_D = (n, d)$ $\qquad Q \xrightarrow{\text{descifr}} Q^d \pmod n$

DH

Se establecen primo grande p y generador g de $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$

A escoge $a \longrightarrow$ publica $g^a \pmod p$

B escoge $b \longrightarrow$ publica $g^b \pmod p$

Ambos pueden calcular $g^{ab} \pmod p$ $\qquad K = g^{ab} \pmod p$

y nadie más

q := número de elementos (número de elementos diferentes)

n := número de coords. elementos

(n, M, d) – código

F := cuerpo de elementos

$\mathcal{C}$:= conjunto de palabras

↳ conjunto de vectores de long. n

K := dimensión mensaje $\mathcal{C}$ (dimensión subespacio)

$M = |\mathcal{C}|$:= número palabras código.

TEOREMA: $d(\mathcal{C}) = d \Rightarrow$ detectar $d-1$ errores.

TEOREMA: $d(\mathcal{C}) = d \Rightarrow$ corregir $\left[\frac{d-1}{2}\right]$ errores.

$w(x)$:= número de coordenadas no nulas.