# CRIPTOGRAFIA

## EN ALGEBRA ABSTRACTA

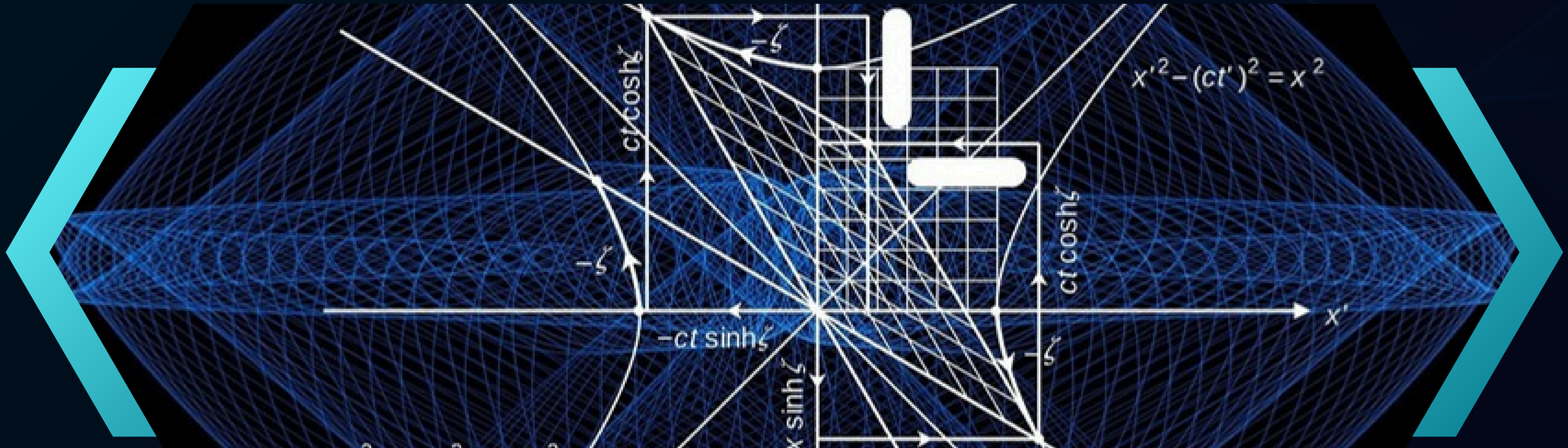


Sebastian Rodriguez, Valentina Hernandez y Camila Patarroyo

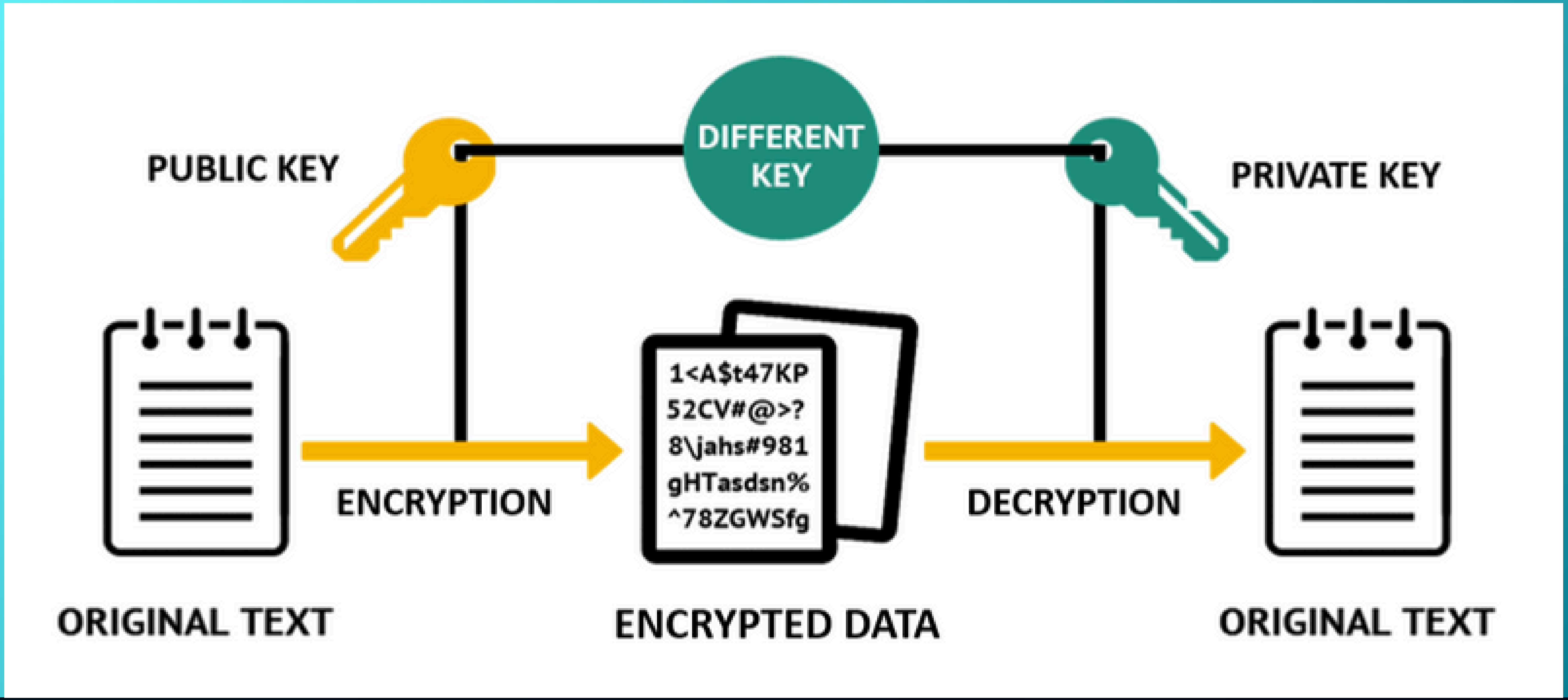
# FUNDAMENTOS MATEMATICOS

**Grupos:** Un grupo es un conjunto con una operación binaria que cumple con cerradura, existencia de un elemento neutro, existencia de inversos y asociatividad. Los grupos abelianos, donde la operación es conmutativa, son especialmente relevantes en criptografía.

**Anillos**: Un anillo es un conjunto con dos operaciones binarias (adición y multiplicación) que cumplen con asociatividad, existencia de un elemento neutro para la adición y distribución de la multiplicación sobre la adición. En criptografía, se utilizan frecuentemente anillos conmutativos, donde la multiplicación es conmutativa.



# ALGORITMO RSA



# EJEMPLO RSA

1.**Seleccionar dos números primos grandes $p$ y $q$:**

$$p=61 \text{ y } q=53$$

2. **Calcular:** $n = p \times q = 61 \times 53 = 3233$

$n$ será parte de la clave pública y privada

3. **Calcular la función totiente:**

$\phi(n) = (p-1) \times (q-1) = (61-1) \times (53-1) = 60 \times 52 = 3120$

$\phi(n)$ es importante para encontrar $e$ y $d$

4. **Elegir un número $e$ tal que $1 < e < \phi(n)$ y $e$ sea coprimo con $\phi(n)$: vamos a elegir $e$=17**

5. **Calcular $d$, el inverso multiplicativo de $e$ módulo $\phi(n)$:**

- Necesitamos encontrar $d$ tal que:

$$d \times e \equiv 1 \mod \phi(n)$$

- Esto se hace usando el algoritmo extendido de Euclides. Para nuestros valores:

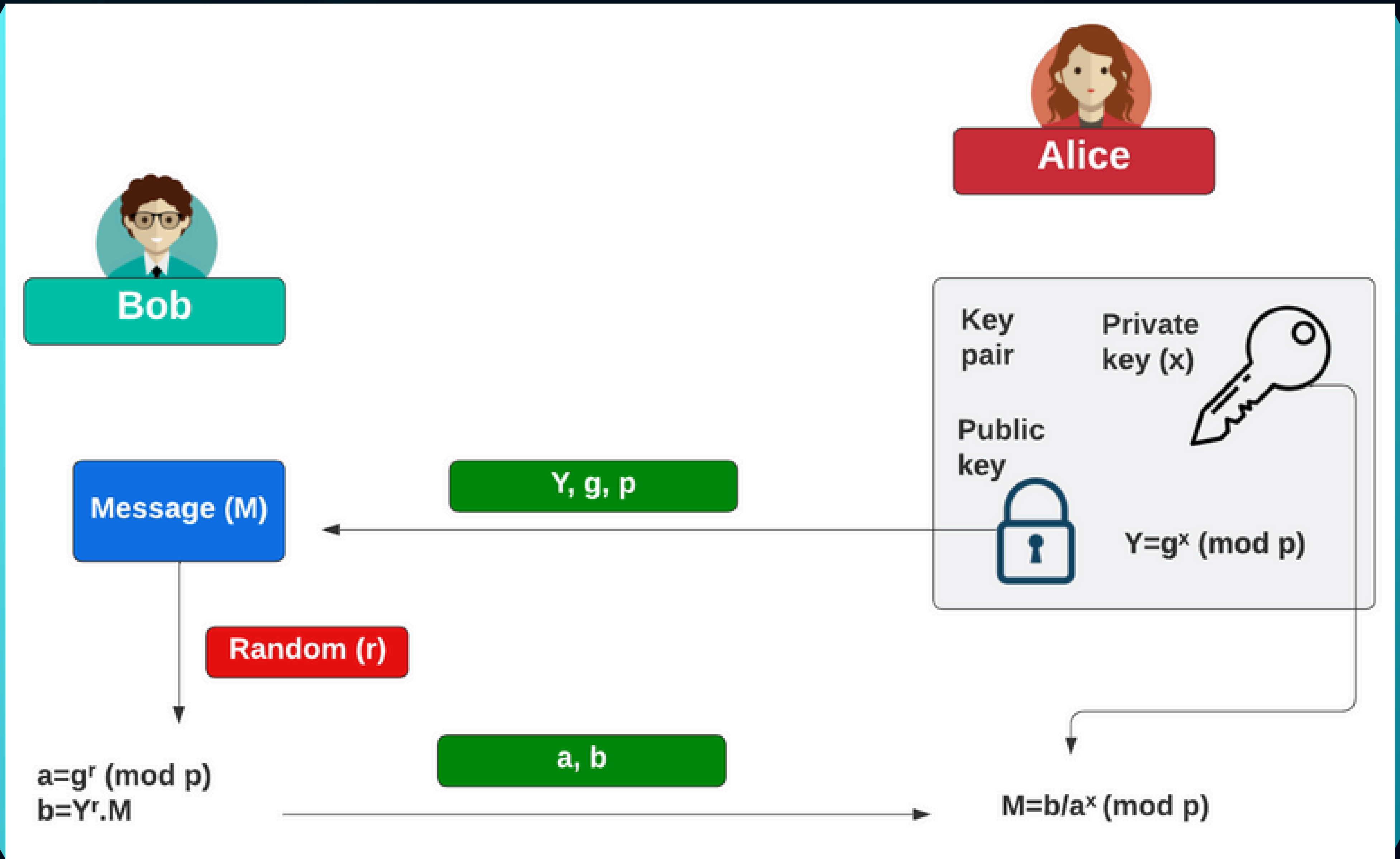
$$d \times 17 \equiv 1 \mod 3120$$

$$d=2753$$

6. **Resumen de las Claves**

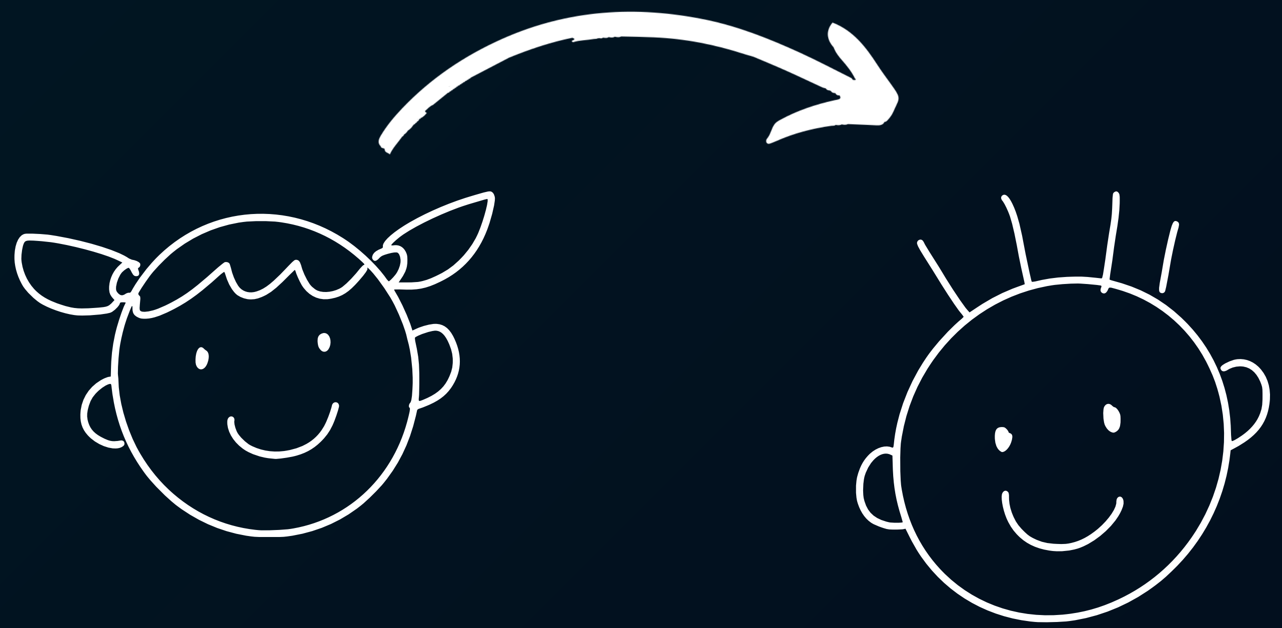
- **Clave pública:** $(e,n)=(17,3233)$
- **Clave privada:** $(d,n)=(2753,3233)$

# ALGORITMO ELGAMAL



# EJEMPLO ELGAMAL

Alicia desea enviar el numero N=2.001 a Bernardo



U = 10

Clave publica de Bernardo $P_B = 99.991$
Generador $\alpha_B = 6$
Clave publica de Bernardo $\beta_B = 77.362$
b = 35

$N_1 = \alpha_B^U \bmod p_B$

$N_1 = 6^{10} \bmod 99.991$

$N_1 = 71.612$

$N_2 = N\, \beta_B^U \bmod p_B$

$N_2 = 2.001 * 77.362 \bmod 99.991$

$N_1 = 71.612$
$N_2 = 33.813$

# EJEMPLO ELGAMAL

$N_3 = N_1^b \mod p_B$

$N_3 = 71.612 \quad \mod 99.991 \; = 50.687$

$N_4 = inv\,(N_3, p_B)$

$N_4 = (50.687\ ,\ 99.991)$

$N_4 = 98.545$

$N = N_2 * N_4 \mod p_B$

$N = 2.001$

# COMPARACION

### Eficiencia

ElGamal puede ser mas eficiente que RSA en terminos de tamaño de clave, pero ambos requieren operaciones de exponenciacion modular.

### Seguridad

RSA se basa en la factorizacion de numeros grandes, mientras que ElGamal se basa en el logaritmo discreto. Ambos son seguros si se eligen correctamente los parametros y se mantienen las claves privadas seguras

### Aplicacion

RSA es muy utilizado en aplicaciones de cifrado y firmas digitales, mientras que ElGamal es popular en protocolos de intercambio de claves y firmas digitales.

# CONCLUSIONES

**RSA** es un algoritmo criptográfico robusto y confiable, ampliamente compatible con protocolos de seguridad como SSL/TLS y PGP. Ofrece una seguridad sólida con longitudes de clave adecuadas y es fácil de implementar.

**ElGamal**, aunque más eficiente en términos de tiempo de cifrado, enfrenta desafíos de adopción y soporte, lo que dificulta su integración en sistemas existentes.

**Comparación de tiempos de cifrado:**
**- RSA: 0.049701 segundos**
**- ElGamal: 0.0075128 segundos**

Finalmente, se elige RSA como el algoritmo principal debido a su seguridad, facilidad de implementación y amplio soporte, a pesar de la mayor eficiencia de ElGamal.

# GRACIAS