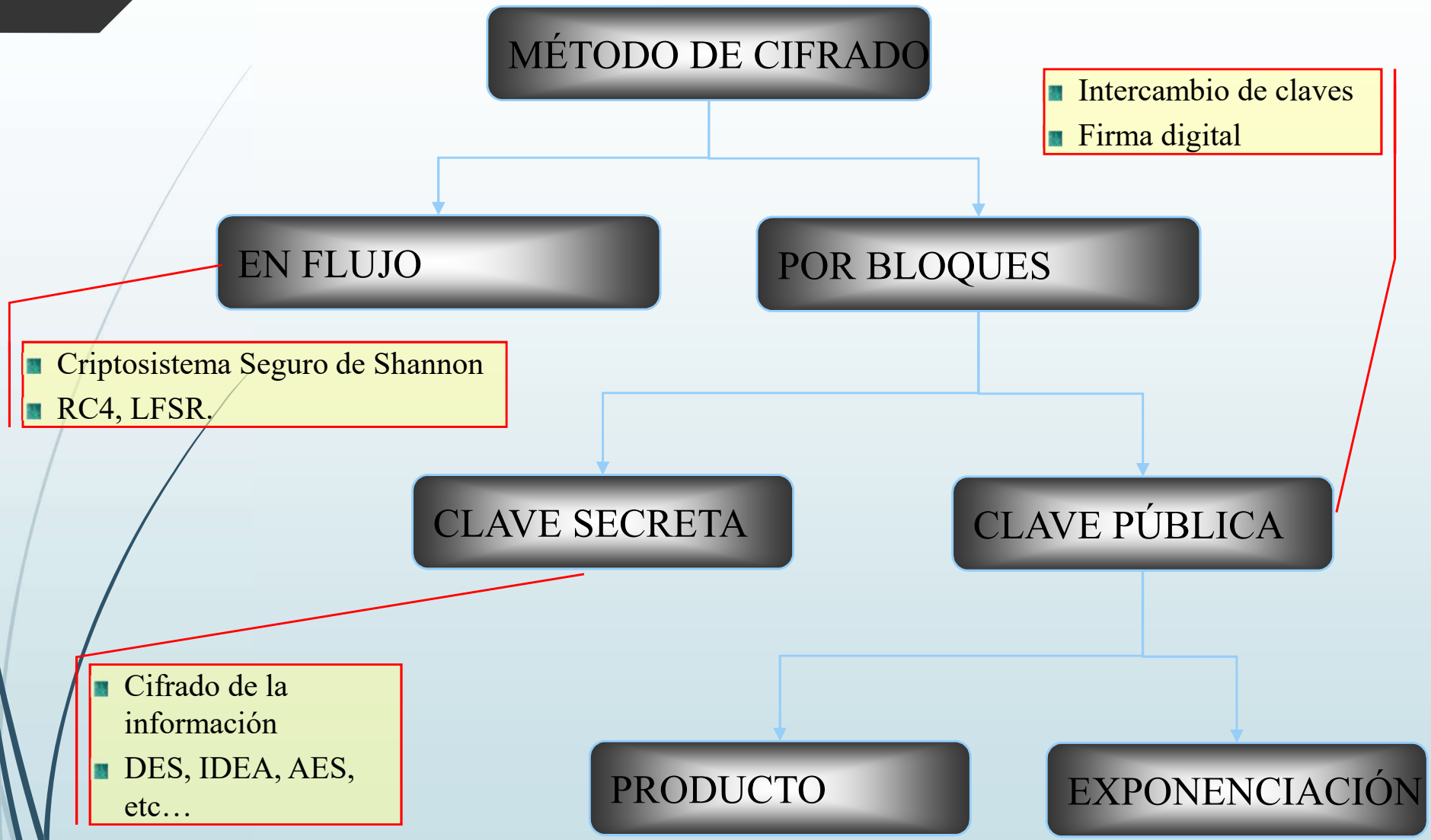
Clasificación de los criptosistemas modernos



5.1 Introducción

- Uno de los mayores inconvenientes que presentan los sistemas de clave secreta cuando existe un gran número de usuarios es que cada par de ellos debe poseer su clave secreta, lo que conlleva gran dificultad en la distribución segura de esas claves.

- Otro gran inconveniente es que no se puede firmar digitalmente el mensaje, con lo que el receptor del mismo no puede estar seguro de su **autenticidad** (o sea, no puede estar seguro de que quien dice que le envía el mensaje sea realmente quien lo ha hecho)

5.1 Introducción

- Un criptosistema de clave pública permite la comunicación cifrada entre dos usuarios sin necesidad de compartir una clave, así como la firma digital de los mensajes.

- Los algoritmos de clave pública, o algoritmos asimétricos, han demostrado su interés para ser empleados en redes de comunicación inseguras (Internet)

- Introducidos por Whitfield Diffie y Martin Hellman a mediados de los años 70, su novedad fundamental con respecto a la criptografía simétrica o de clave secreta es que las claves no son únicas, sino que forman pares con la propiedad de que una es capaz de descifrar lo que ha sido cifrado por la otra.

5.1 Introducción

- Los algoritmos **asimétricos**, por lo general, basan su seguridad en el enfrentamiento del atacante a **problemas matemáticos que requieren mucha computación**.

- Emplean, generalmente, longitudes de clave mucho mayores que los simétricos.
  - Por ejemplo, mientras que para algoritmos simétricos se considera **segura una clave de 128 bits**, para algoritmos asimétricos (si exceptuamos aquellos basados en curvas elípticas) se recomiendan **claves de al menos 1024 bits**.

- La complejidad de cálculo que comportan los hace **considerablemente más lentos** que los algoritmos de cifrado simétricos.

- ***En la práctica*** *los métodos asimétricos* ***se emplean únicamente para cifrar la clave de sesión (simétrica)*** *de cada mensaje o transacción particular*.

5.1 Introducción

- **Fijadas las dos claves de cada usuario** como clave pública y clave privada.
- **La clave privada** deberá ser custodiada por el usuario y es imprescindible que se mantenga en **secreto**.
- **La clave pública**, por el contrario, **se publicará junto con la identidad del usuario**.
- Así, cuando se quiera enviar un mensaje seguro a un usuario se hará uso de la clave pública, que se utilizará para cifrar el mensaje a enviar.

5.1 Introducción

- El resultado de esta operación será el texto cifrado que sólo el propietario de la clave privada correspondiente a esa clave pública podrá descifrar.

- Estas claves tienen características matemáticas especiales.
  - **Se generan siempre a la vez**, por parejas, **estando cada una de ellas ligada intrínsecamente a la otra**,
  - de tal forma que **si dos claves públicas son diferentes**, entonces **sus claves privadas asociadas también lo son** y **viceversa**.

5.1 Introducción

- Los algoritmos de clave pública están basados en funciones matemáticas **fáciles de resolver en un sentido**, pero muy **complicadas de realizar en sentido inverso**, salvo que se conozca alguna trampa.

- Ambas **claves**, pública y privada, **están relacionadas matemáticamente**, pero esta **relación debe ser lo suficientemente compleja** como para que resulte muy difícil obtener una a partir de la otra.

- Este es el motivo por el que normalmente estas **claves** no las **elige** el usuario, si no que lo hace **un algoritmo específico para ello**.

5.1 Introducción

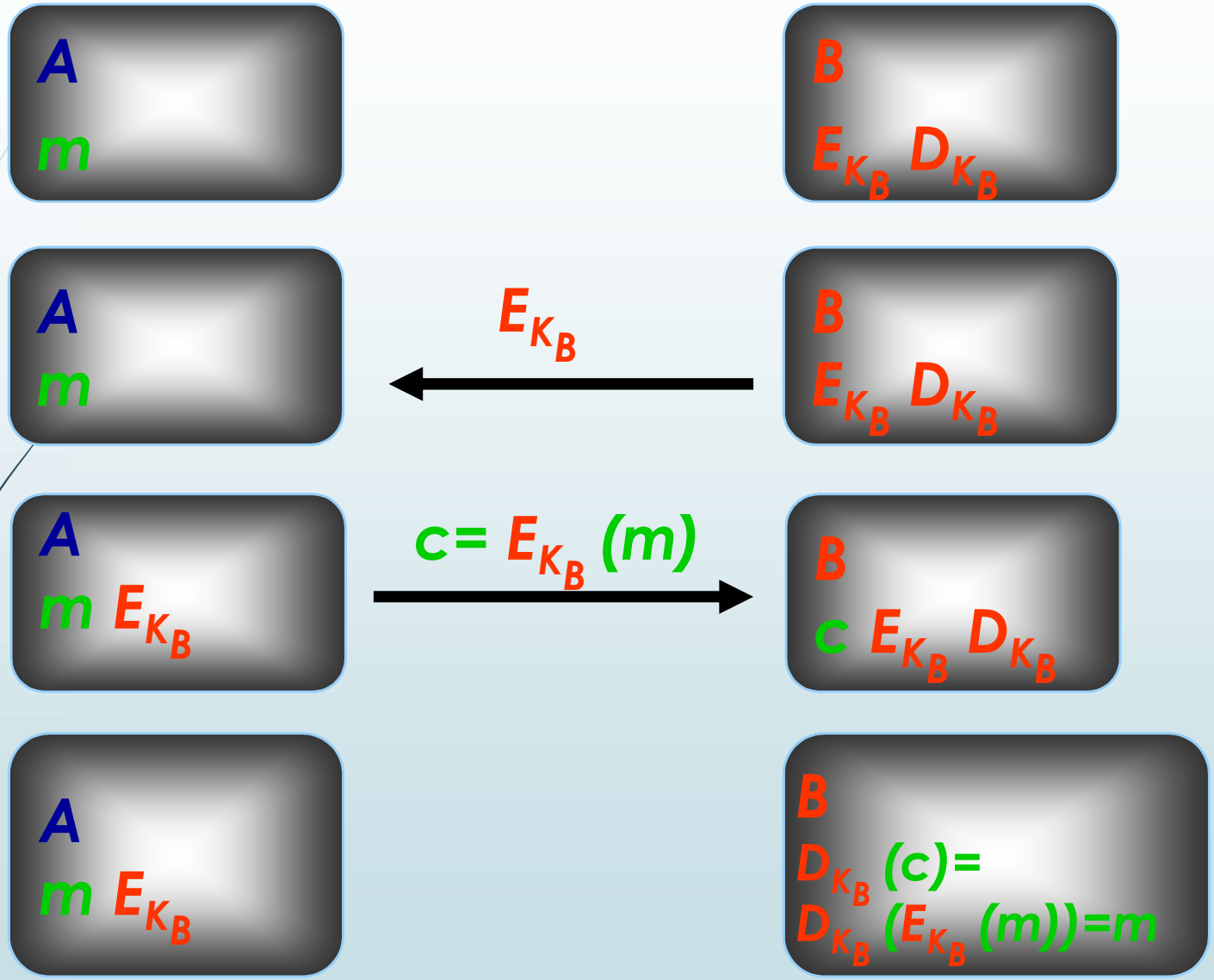
- En este tipo de ciptosistemas, para enviar un mensaje con seguridad, el emisor A cifra el mismo con la clave pública del receptor B y lo envía por el medio inseguro.

- Este mensaje está totalmente protegido en su viaje, ya que sólo se puede descifrar con la clave privada correspondiente, conocida solamente por B.

- Al llegar el mensaje cifrado a su destino, el receptor usa su clave privada para obtener el mensaje en claro.

5.1 Introducción

CRIPTOSISTEMA DE CLAVE PÚBLICA



5.1 Introducción

- Una variación de este sistema se produce cuando es el emisor (A) el que cifra un texto con su clave privada, enviando por el medio inseguro tanto el mensaje en claro como el cifrado.

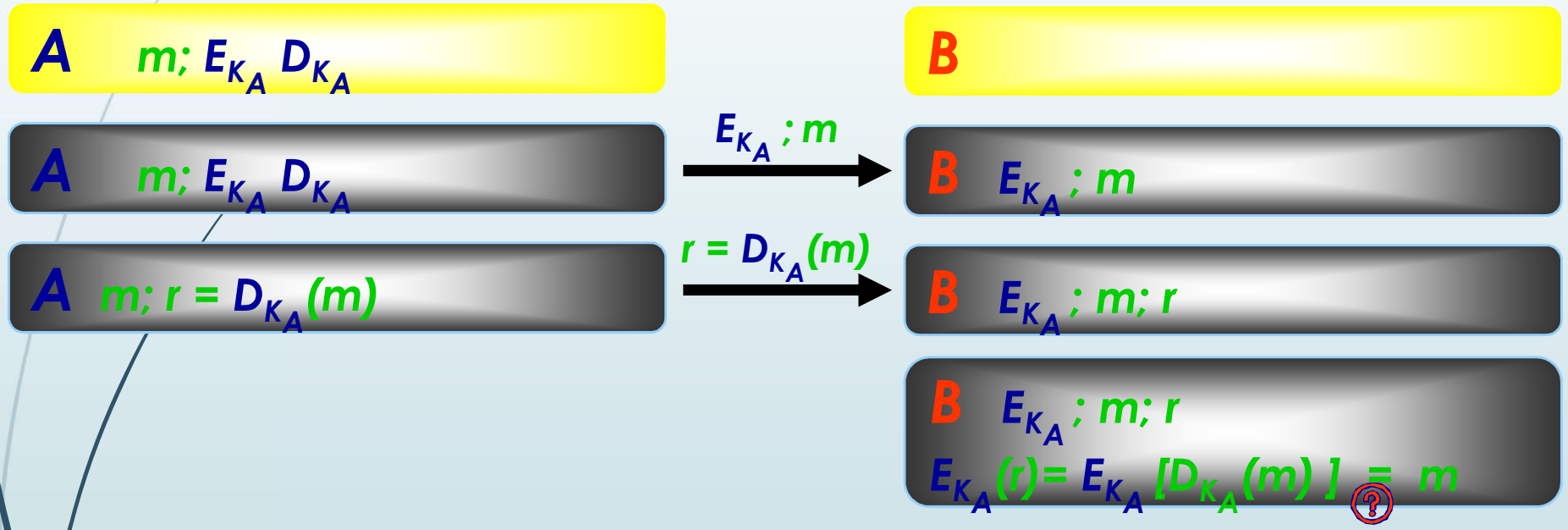
- Así, cualquier receptor B del mismo puede comprobar que el emisor ha sido A, y no otro que lo suplante, con tan sólo descifrar el texto cifrado con la clave pública de A y comprobar que coincide con el texto sin cifrar.

- Como sólo A conoce su clave privada, B puede estar seguro de la autenticidad del emisor del mensaje.

- Este sistema de autentificación de denomina **firma digital**.

5.1 Introducción

FIRMA DIGITAL SIN CIFRADO



5.1 Introducción

PRINCIPAL VENTAJA E INCONVENIENTE DE LA CRIPTOGRAFÍA DE CLAVE PÚBLICA

- La principal ventaja de los criptosistemas de clave pública frente a los de clave secreta es que la clave pública y el algoritmo de cifrado son o pueden ser de dominio público y no es necesario poner en peligro la clave privada enviándola por medios potencialmente inseguros, ya que ésta debe permanecer siempre oculta y en poder, únicamente, de su propietario.

- El principal inconveniente que presentan estos criptosistemas frente a los de clave secreta es que son mucho más lentos, por lo que, generalmente, se usan para el envío seguro de la clave de cifrado del criptosistema de clave secreta utilizado para el cifrado de la información.

5.1 Introducción

- En muchas ocasiones, se implementan sistemas criptográficos mixtos,
  - en los que se usa la clave pública del receptor para cifrar una clave simétrica que se usará en el proceso de comunicación cifrada.

- De esta forma se aprovechan las ventajas de ambos sistemas, usando el sistema asimétrico para el envío de la clave sensible y el simétrico, con mayor velocidad de proceso, para el envío masivo de datos.

- El primer sistema de clave pública que apareció fue el de Diffie-Hellman, en 1976, y fue la base para el desarrollo de los que después aparecieron, entre los que cabe destacar RSA, que es el más utilizado hoy día.

5.2 La problemática de la distribución de claves

- El problema de la distribución de claves ha acosado a los criptógrafos a lo largo de la historia.
  - Por ejemplo, durante la Segunda Guerra Mundial, el Alto Mando alemán tenía que distribuir el libro mensual de claves del día a todos sus operadores de la Enigma, lo que suponía un enorme problema logístico.
  - Asimismo, los submarinos, que tendían a pasar extensos períodos lejos de la base, tenían que obtener de alguna manera un suministro regular de claves.

- **No importa lo seguro que sea un cifrado** en teoría, en la **práctica puede ser socavado por el problema de la distribución de claves**.

5.2 La problemática de la distribución de claves

- La distribución de claves podría parecer un tema anodino y trivial, pero se convirtió en el principal problema para los criptógrafos tras la posguerra.

- Si dos partes querían **comunicarse de manera segura**, debían **recurrir** a **una tercera parte** para distribuir la clave, y, sin lugar a dudas, éste se convirtió en **el eslabón más débil** de la **cadena de seguridad**.

5.2 La problemática de la distribución de claves

- A pesar de las afirmaciones que aseguraban que **el problema de la distribución de claves no tenía solución**, surgió un grupo de personas independiente que propuso una solución brillante a **mediados de los años setenta**.

- Esto significaría un gran avance, aunque los ordenadores transformaron la aplicación de las claves, **la mayor revolución de la criptografía del siglo XX** ha sido el **desarrollo de técnicas** para **superar el problema de la distribución de claves**.

5.2 La problemática de la distribución de claves

- Whitfield Diffie estaba particularmente interesado en el problema de la distribución de claves y se dio cuenta de que quien lograra encontrar una solución pasaría a la historia como uno de los mejores criptógrafos de todos los tiempos.

- Diffie se adelantó a su tiempo e imaginó un mundo con un sistema de información interconectado, entonces se preguntó cómo dos personas podrían enviarse un mensaje cifrado en una red global en la que cualquiera podía estar escuchando.

- **El problema anterior obsesionó a Diffie**, llevándole a elaborar diversas estrategias para atacar el problema de la distribución de claves, pero todas sus ideas eran muy tentativas y la audiencia que tuvo en su momento se mostró bastante escéptica ante ellas.

5.2 La problemática de la distribución de claves

- La suerte le cambiaría a Diffie cuando supo que alguien trabajaba en la resolución del problema de la distribución de claves.

- Inmediatamente salió en busca de esta persona y, después de recorrer más de 5.000 kilómetros, encontró a **Martin Hellman**.

- Una vez establecida esta alianza, les quedó claro que el problema era una situación clásica de **círculo vicioso**.
  - Si dos personas quieren intercambiar un mensaje secreto por teléfono, el emisor debe cifrarlo.
  - Para cifrar el mensaje secreto, el emisor debe usar una clave, que es en sí misma es un secreto, de modo que entonces existe el problema de transmitir la clave secreta al receptor para transmitir el mensaje secreto.

- En resumen, **antes de que dos personas puedan intercambiar un secreto (el mensaje) deben ya compartir uno (la clave).**

5.2 La problemática de la distribución de claves

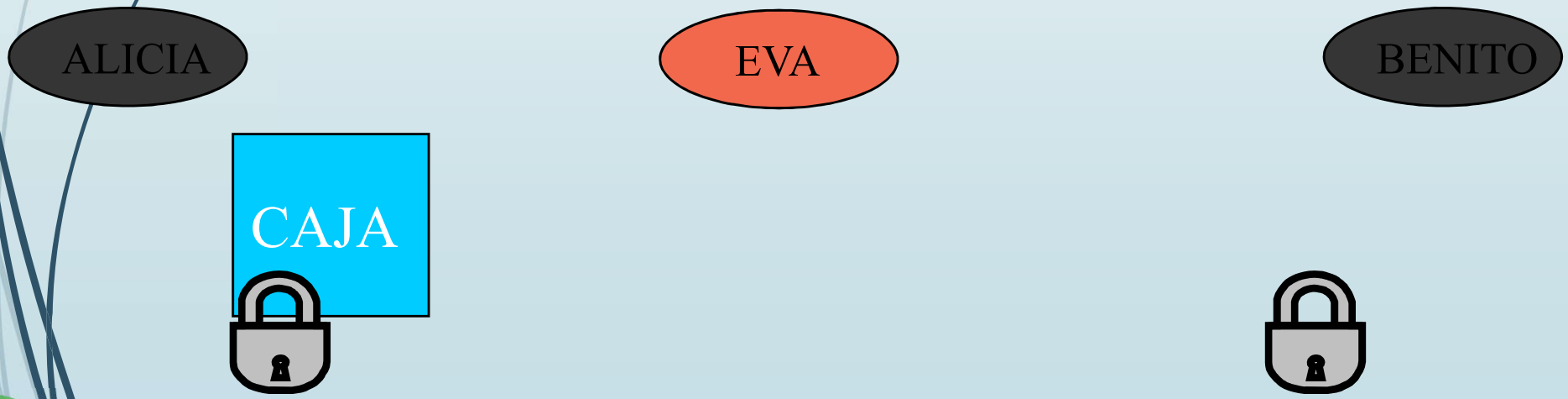
- Los nombres de Alicia, Benito y Eva (Alice, Bob y Eve) se han convertido en tres personajes ficticios estándar en las discusiones sobre criptografía, siendo Alicia y Benito el emisor y receptor, y Eva la persona que intentará saber de qué hablan.

- Estos tres serán los protagonistas de una primera idea que haría tomar un rumbo nuevo al análisis del problema.

5.2 La problemática de la distribución de claves

EJEMPLO GRÁFICO DIFFIE-HELLMAN

- Imaginemos la siguiente situación.
- Alicia quiere enviar un mensaje personal a Benito,
- Para ello mete su mensaje secreto en una caja de hierro, la cierra con candado y se la envía a Benito.
- Cuando llega la caja, Benito añade su propio candado y vuelve a enviar la caja a Alicia



5.2 La problemática de la distribución de claves

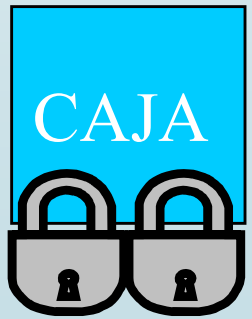
EJEMPLO GRÁFICO DIFFIE-HELLMAN

- Imaginemos la siguiente situación.
- Alicia quiere enviar un mensaje personal a Benito,
- Para ello mete su mensaje secreto en una caja de hierro, la cierra con candado y se la envía a Benito.
- Cuando llega la caja, Benito añade su propio candado y vuelve a enviar la caja a Alicia
- Cuando Alicia recibe la caja, ahora está cerrada con dos candados. Ella retira su propio candado, dejando que sólo el candado de Benito cierre la caja.

ALICIA

EVA

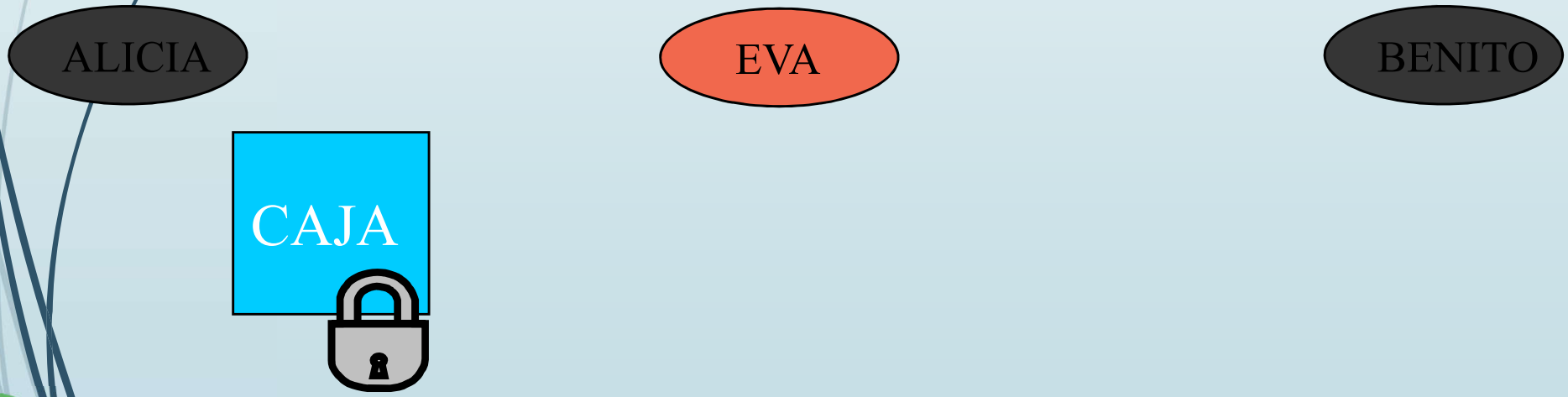
BENITO



5.2 La problemática de la distribución de claves

EJEMPLO GRÁFICO DIFFIE-HELLMAN

- Imaginemos la siguiente situación.
- Alicia quiere enviar un mensaje personal a Benito,
- Para ello mete su mensaje secreto en una caja de hierro, la cierra con candado y se la envía a Benito.
- Cuando llega la caja, Benito añade su propio candado y vuelve a enviar la caja a Alicia
- Cuando Alicia recibe la caja, ahora está cerrada con dos candados. Ella retira su propio candado, dejando que sólo el candado de Benito cierre la caja.
- Finalmente, vuelve a enviar la caja a Benito, y éste puede ahora retirar su candado y obtener el mensaje contenido en la caja.



5.2 La problemática de la distribución de claves

PROTOCOLO CLAVE PÚBLICA

- Imaginemos la siguiente situación.
- Alicia quiere enviar un mensaje personal a Benito.
- Para ello, Benito le envía su candado abierto.

ALICIA

BENITO

5.2 La problemática de la distribución de claves

PROTOCOLO CLAVE PÚBLICA

- Imaginemos la siguiente situación.
- Alicia quiere enviar un mensaje personal a Benito.
- Para ello, Benito le envía su candado abierto.
- Alicia mete su mensaje secreto en una caja de hierro, la cierra con el candado de Benito y se la envía a Benito.

5.2 La problemática de la distribución de claves

PROTOCOLO CLAVE PÚBLICA

- Imaginemos la siguiente situación.
- Alicia quiere enviar un mensaje personal a Benito.
- Para ello, Benito le envía su candado abierto.
- Alicia mete su mensaje secreto en una caja de hierro, la cierra con el candado de Benito y se la envía a Benito.
- Finalmente Benito abre su candado y puede obtener el mensaje contenido en la caja.

5.2 La problemática de la distribución de claves

- Las implicaciones de esta historia son enormes. Demuestra que **un mensaje secreto se puede intercambiar de manera segura entre dos personas sin que tengan necesariamente que intercambiar una clave**.

- Aunque el enfoque de la **caja cerrada con dos candados no funcionaba** en la criptografía de la **vida real**, **inspiró a Diffie y Hellman** a buscar un **método práctico** para resolver el problema de la distribución de claves.

- Para ello, acabarían buscando **funciones que no fueran reversibles**, es decir, funciones de una sola vía.

- La **aritmética modular** es un área de las matemáticas muy rica en funciones de una sola vía.

5.3 Intercambio de clave Diffie-Hellman

- **Después de dos años** concentrándose en la aritmética modular y las funciones de un sola vía, se empezaron a obtener frutos.

- En la **primavera de 1976** Hellman dio con la estrategia para resolver el problema.

- La idea de Hellman se basaba en una función de una sola vía de la forma

$$\alpha^x \bmod p$$

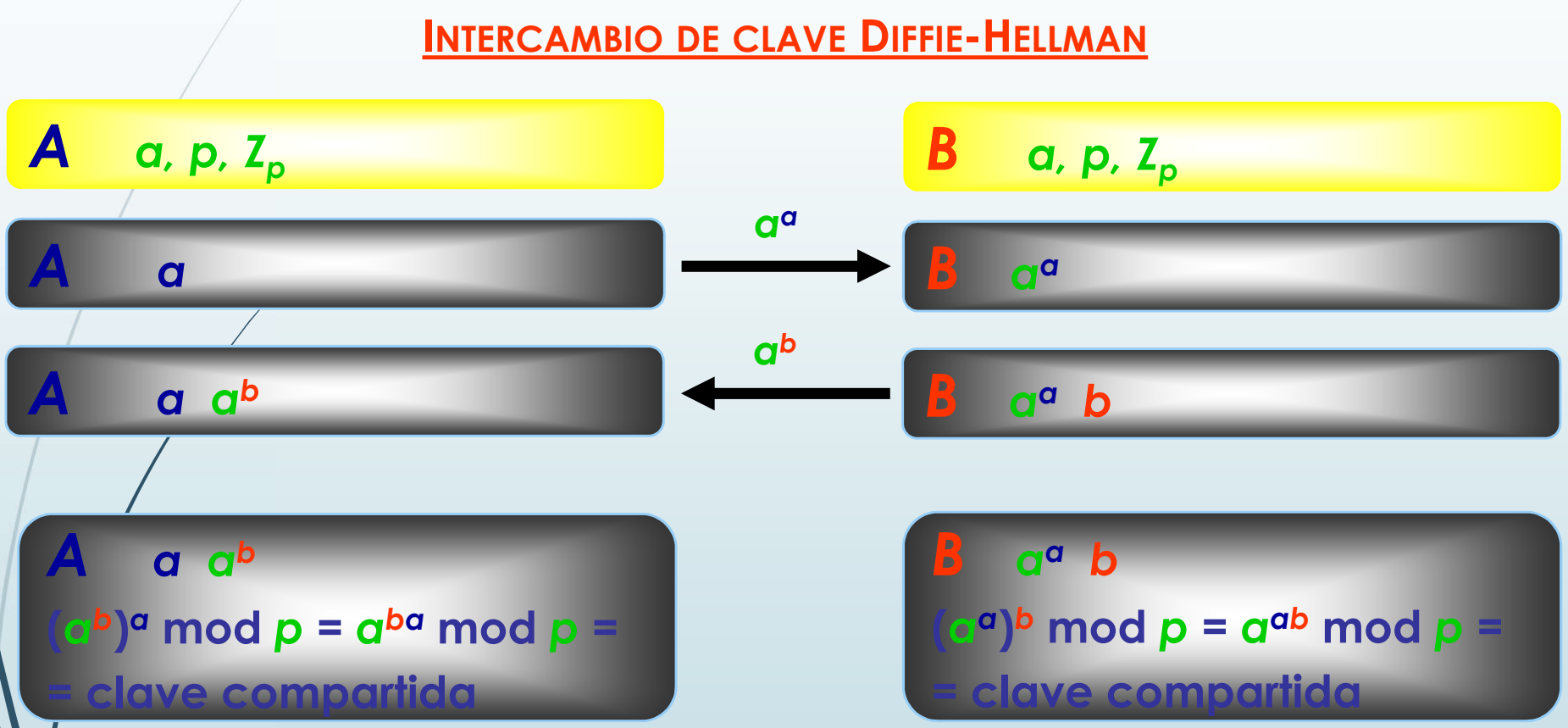
- Inicialmente **A**licia y **B**enito acuerdan α y p sin importar que **E**va esté escuchando el canal y obtenga también estos dos números. A partir de esta idea tan sencilla se obtuvieron resultados sorprendentes que revolucionarían el mundo de la criptografía y de las comunicaciones.

5.3 Intercambio de clave Diffie-Hellman

INTERCAMBIO DE CLAVE DE DIFFIE Y HELLMAN

- ***A*** y ***B*** seleccionan un número primo p y un generador α de $\mathbb{Z}_p$, ambos valores públicos
- ***A*** genera un número aleatorio ***a*** y envía a ***B*** $\alpha^a \bmod p$
- ***B*** genera un número aleatorio ***b*** y envía a ***A*** $\alpha^b \bmod p$
- ***B*** calcula $(\alpha^a)^b \bmod p = \alpha^{ab} \bmod p$
- ***A*** calcula $(\alpha^b)^a \bmod p = \alpha^{ba} \bmod p$
- El secreto compartido por ***A*** y B es el valor $\alpha^{ab} \bmod p$

5.3 Intercambio de clave Diffie-Hellman



5.3 Intercambio de clave Diffie-Hellman

GRUPO

Definición:

Un grupo es un conjunto de elementos sobre los que se define un operador que verifica las propiedades asociativa, identidad (existencia de un elemento neutro) e invertibilidad (cada elemento posee inverso).

- Si el operador verifica la propiedad conmutativa se dice que el grupo es conmutativo o abeliano.

Ejemplo

- Z_p, con p primo es un grupo conmutativo en el que el neutro es 1 (el operador es la multiplicación módulo p).

5.3 Intercambio de clave Diffie-Hellman

GRUPO CÍCLICO - GENERADOR

Definición:

Un grupo se denomina cíclico cuando puede ser generado por un solo elemento del mismo.

- Dado un número primo p, el conjunto $\mathbb{Z}_p$ formado por los enteros positivos menores que p es un grupo cíclico y finito con respecto de la multiplicación módulo p.

- Esto quiere decir que existe al menos un valor $\alpha \in \mathbb{Z}_p$ tal que cualquier otro entero $\beta \in \mathbb{Z}_p$ se puede expresar de la forma $\beta = \alpha^i \bmod p$ para algún entero i tal que $0 < i < p$.

- El elemento α se denomina generador, elemento primitivo o raíz primitiva del grupo $\mathbb{Z}_p$.

5.3 Intercambio de clave Diffie-Hellman

EJEMPLO DE GENERADORES

$Z_5 = \{0,1,2,3,4\}$

α=**2** es generador de $\mathbb{Z}_5$

$\alpha^2 = 4 \bmod 5 = 4$

$\alpha^3 = 8 \bmod 5 = 3$

$\alpha^4 = 16 \bmod 5 = 1$

$\alpha^5 = 32 \bmod 5 = 2$

α=**3** es generador de $\mathbb{Z}_5$

$\alpha^2 = 9 \bmod 5 = 4$

$\alpha^3 = 27 \bmod 5 = 2$

$\alpha^4 = 81 \bmod 5 = 1$

$\alpha^5 = 243 \bmod 5 = 3$

α=**4 NO** es generador de $\mathbb{Z}_5$

$\alpha^2 = 16 \bmod 5 = 1$

$\alpha^3 = 64 \bmod 5 = 4$

$\alpha^4 = 256 \bmod 5 = 1$

$\alpha^5 = 1024 \bmod 5 = 4$

5.3 Intercambio de clave Diffie-Hellman

FUNCIÓN DE EULER

Definición

Se define la **función de Euler**, Φ, como la función natural de variable natural tal que para un número natural n

$$\Phi(n)=card\{i \in N \,/\, 1 \leq i < n \text{ y } mcd(i,n)=1\}$$

es decir, $\Phi(n)$ es igual al número de números naturales menores n, primos con n.

Ejemplo

- $\Phi(8) = 4$ (ya que son primos con 8 los números 1, 3, 5 y 7)
- $\Phi(11) = 10$ (ya que son primos con 11 los números 1, 2, 3, 4, 5, 6, 7, 8, 9 y 10)
- Si p es primo entonces $\Phi(p) = p-1$

5.3 Intercambio de clave Diffie-Hellman

FUNCIÓN DE EULER

Proposición

Si p y q son dos números primos entre sí

$$\Phi(p\,q)= \Phi(p)\,\Phi(q)$$

Corolario

Si p y q son dos números primos

$$\Phi(p\,q)= (p-1)\,(q-1)$$

Ejemplo

- $\Phi(55) = \Phi(5\cdot 11) = 4\cdot 10 = 40$

5.3 Intercambio de clave Diffie-Hellman

FUNCIÓN DE EULER

Proposición

Si p es un número primo y $r \in \mathbb{Z}^+$ entonces

$$\Phi(p^r) = p^r (p-1)$$

Teorema

Si $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ es la descomposición en factores primos de un entero positivo n, $\Phi(n) = p_1^{r_1-1}(p_1-1)\, p_2^{r_2-1}(p_2-1) \cdots p_k^{r_k-1}(p_k-1)$

Ejemplo

- $\Phi(275) = \Phi(5^2 \cdot 11) = 5^{(2-1)}(5-1)\ 11^0\ (11-1) = 200$

5.3 Intercambio de clave Diffie-Hellman

PROPIEDADES DE GENERADORES

- El número de generadores de un grupo cíclico $\mathbb{Z}_n$ es $\Phi(\Phi(n))$
  - Ejemplo:

    Z_5 tiene $\Phi(\Phi(5)) = \Phi(4) = 2$ generadores

    (como se ha visto en el ejemplo anterior, son α=**2** y α=**3** mientras que α=**4** no lo es)

  - $\alpha \in Z_n$ es generador si y solo si
    para cada primo, p, divisor de $\Phi(n)$ se cumple $\alpha^{\Phi(n)/p} \bmod n \neq 1$

  - Ejemplo en Z_5:

    $\Phi(5)=4$; divisores primos de $\Phi(5)$: $\{2\}$;

    $\mathbf{2}^{\Phi(5)/2} \bmod 5 = 2^2 \bmod 5 = 4 \neq 1$; $\mathbf{3}^{\Phi(5)/2} \bmod 5 = 3^2 \bmod 5 = 4 \neq 1$;

    $\mathbf{4}^{\Phi(5)/2} \bmod 5 = 4^2 \bmod 5 = 1$;

5.3 Intercambio de clave Diffie-Hellman

EJEMPLO DE INTERCAMBIO DE CLAVE DH

p=1999 es primo y α = 33 es generador de $\mathbb{Z}_{1999}$, como se comprueba a continuación:

$\Phi(1999)=1998$; divisores primos de $\Phi(1999)$: $\{2,3,37\}$;

$33^{\Phi(1999)/2} \bmod 1999 = 33^{999} \bmod 1999 = 1998 \neq 1$
$33^{\Phi(1999)/3} \bmod 1999 = 33^{666} \bmod 1999 = 1190 \neq 1$
$33^{\Phi(1999)/37} \bmod 1999 = 33^{54} \bmod 1999 = 870 \neq 1$

5.3 Intercambio de clave Diffie-Hellman

EJEMPLO DE INTERCAMBIO DE CLAVE DH

Alicia (***A***) y Benito (***B***) van a intercambiar una clave de sesión dentro del grupo multiplicativo $\mathbb{Z}_{1999}$, con $\alpha = 33$.
El usuario A elige ***a*** = 47 y el usuario ***B*** elige ***b*** = 117.

1. ***A*** calcula $\alpha^a \bmod p = 33^{47} \bmod 1.999 = 1.343$ y se lo envía a ***B***.
2. ***B*** calcula $\alpha^b \bmod p = 33^{117} \bmod 1.999 = 1.991$ y se lo envía a ***A***.
3. ***B*** recibe 1.343 y calcula $1.343^{117} \bmod 1.999 = 1.506$.
4. ***A*** recibe 1.991 y calcula $1.991^{47} \bmod 1.999 = 1.506$.

La clave de sesión compartida por (***A***) y (***B***) es $1.506 = 10111100010_{(2)}$

5.3 Intercambio de clave Diffie-Hellman

EXPONENCIACIÓN RÁPIDA

Para calcular, por ejemplo, 8^{17} mod 899 debemos actuar del siguiente modo ($17=10001_{(2)}$)

$8^{17} \bmod 899 = 8^{16+1} \bmod 899 =$
$= 8^{16}\ 8 \bmod 899 =$
$= (((8^2)^2)^2)^2\ 8 \bmod 899 =$
$= (((64)^2)^2)^2\ 8 \bmod 899 =$
$= ((4096)^2)^2\ 8 \bmod 899 =$
$= ((500)^2)^2\ 8 \bmod 899 =$ (4096 mod 899 =500)
$= (250000)^2\ 8 \bmod 899 =$
$= (78)^2\ 8 \bmod 899 =$ (250000 mod 899 =78)
$= 6084\ 8 \bmod 899 =$
$= 690\ 8 \bmod 899 =$ (6084 mod 899 =690)
$= 5520 \bmod 899 =$
$= 126$

5.3 Intercambio de clave Diffie-Hellman

EJEMPLO DE INTERCAMBIO DE CLAVE DH

En el ejemplo D-H, para calcular 33^{47} mod 1999 debemos actuar del siguiente modo, dado que $47=101111_{(2)}$

$33^{47} \bmod 1999 = 33^{32+8+4+2+1} \bmod 1999 =$

$= 33^{32}$	33^8	33^4	33^2	$33 \bmod 1999$	$=$
$= ((((33^2)^2)^2)^2)^2$	$(((33^2)^2)^2$	$(33^2)^2$	33^2	$33 \bmod 1999$	$=$
$= ((((1089)^2)^2)^2)^2$	$((1089)^2)^2$	$(1089)^2$	1089	$33 \bmod 1999$	$=$
$= (((514)^2)^2)^2$	$(514)^2$	514	1089	$33 \bmod 1999$	$=$
$= ((328)^2)^2$	328	514	1089	$33 \bmod 1999$	$=$
$= (1637)^2$	328	514	1089	$33 \bmod 1999$	$=$
$= 1109$	328	514	1089	$33 \bmod 1999$	$=$
$= 1109$	328	514	1954	$\bmod 1999$	$=$
$= 1109$	328	858		$\bmod 1999$	$=$
$= 1109$	1564			$\bmod 1999$	$=$
$= 1343$					

5.3 Intercambio de clave Diffie-Hellman

EJEMPLO DE INTERCAMBIO DE CLAVE DH

En la práctica $33^{47} \bmod 1999$ se puede calcular del siguiente modo:

$47 = 101111_{(2)}$

$33 \bmod 1999 = 33$ **1**

$33^2 \bmod 1999 = 1089 \bmod 1999 = 1089$ **1**

$33^4 \bmod 1999 = 1089^2 \bmod 1999 = 514$ **1**

$33^8 \bmod 1999 = 514^2 \bmod 1999 = 328$ **1**

$33^{16} \bmod 1999 = 328^2 \bmod 1999 = 1637$ **0**

$33^{32} \bmod 1999 = 1637^2 \bmod 1999 = 1109$ **1**

Ahora solo queda multiplicar las potencias con **1**

$(33^{47} \bmod 1999 = 33^{1+2+4+8+32} \bmod 1999 = 33\ 33^2\ 33^4\ 33^8\ 33^{32} \bmod 1999)$

$33 \cdot 1089 \bmod 1999 = 1954$

$1954 \cdot 514 \bmod 1999 = 858$

$858 \cdot 328 \bmod 1999 = 1564$

$1564 \cdot 1109 \bmod 1999 = 1343$

Alice y Bob desean intercambiar una clave de sesión mediante el protocolo Diffie-Hellman. Para ello acuerdan un número primo p=503 y un generador α=399 de $\mathbb{Z}_{503}$. Alice genera aleatoriamente un número privado a=257 y Bob otro número privado b=320.

a) Comprueba que el generador se ha elegido correctamente.
b) ¿Qué valor envía Alice a Bob?
c) ¿Qué valor envía Bob a Alice?
d) ¿Qué clave comparten?