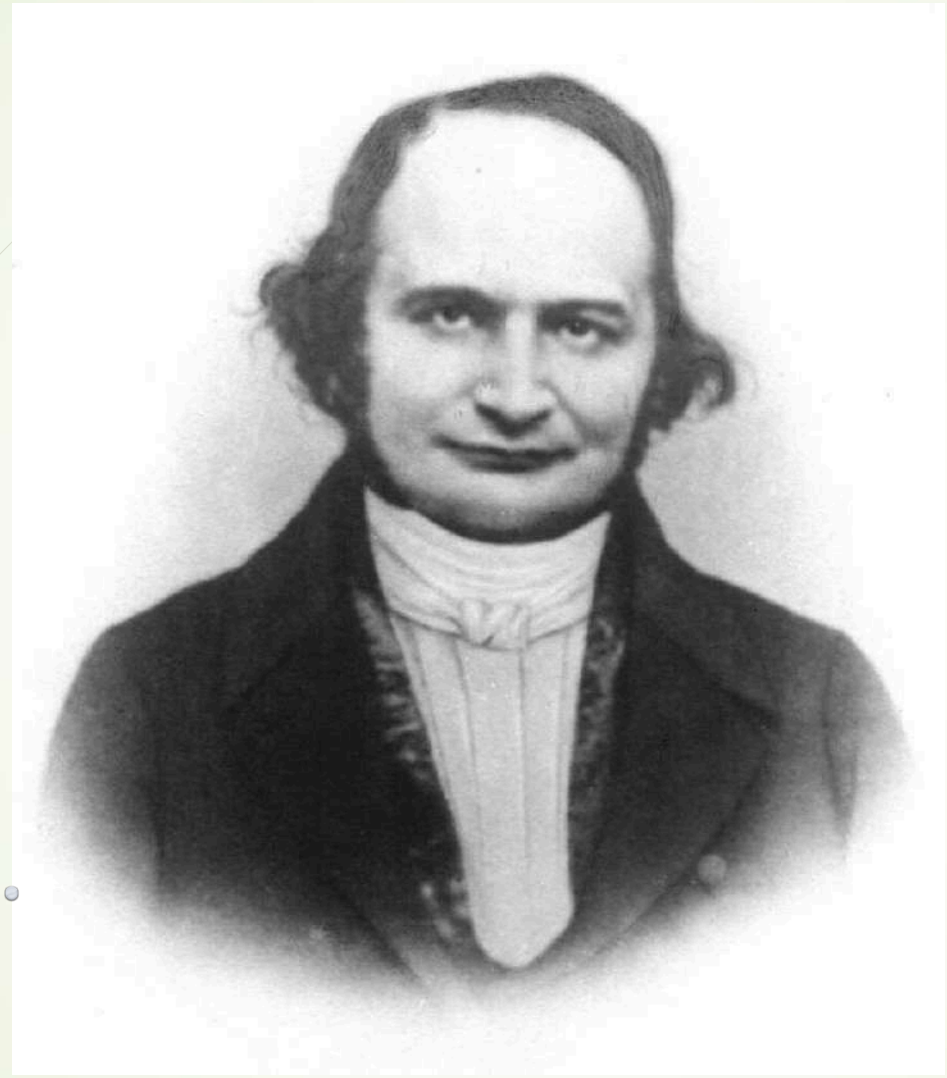
Clase 21



C. G. Jacobi

- Veamos ahora la demostración de las propiedades de reciprocidad del símbolo de Jacobi:
- (a) Probémosla por inducción sobre el número de divisores primos de b. Sea $b = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ donde los p_i son primos (no necesariamente todos diferentes) y $r \geqq 1$.
- Si r = 1, b es primo y $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$ es una propiedad ya demostrada del símbolo de Legendre.
- Si r > 1, suponemos por hipótesis de inducción que la propiedad es cierta para el caso de r-1 divisores primos, por lo tanto si $c = b/p_r \Rightarrow \left(\frac{-1}{c}\right) = (-1)^{\frac{c-1}{2}}$
- Por otro lado, también se tiene (por ser p_r primo): $\left(\frac{-1}{p_r}\right) = (-1)^{\frac{p_r-1}{2}}$
- De aquí, por el Lema 1: $\left(\frac{-1}{b}\right) = \left(\frac{-1}{c}\right) \cdot \left(\frac{-1}{p_r}\right) = (-1)^{\frac{c-1}{2}} \cdot (-1)^{\frac{p_r-1}{2}} = (-1)^{\frac{c-1}{2}+\frac{p_r-1}{2}} = (-1)^{\frac{b-1}{2}}$. Esto acaba la demostración por inducción en r.

- (b) Aplicamos inducción en r, el número de divisores primos de b. Para r=1, es una propiedad del símbolo de Legendre equivalente a un resultado ya demostrado.
- Si $b = p_1 \cdot p_2 \cdot \ldots\ldots \cdot p_r$ con $r > 1$, sea $c = b / p_r$. Por hipótesis de inducción suponemos que la propiedad es cierta para el caso de r-1 divisores, con lo cual es cierta para c, es decir: $\left(\frac{2}{c}\right) = (-1)^{\frac{c^2-1}{8}}$.
- También sabemos (por ser p_r primo) que: $\left(\frac{2}{p_r}\right) = (-1)^{\frac{p_r^2-1}{8}}$. De aquí, por el lema 2: $\left(\frac{2}{b}\right) = \left(\frac{2}{c}\right) \cdot \left(\frac{2}{p_r}\right) = (-1)^{\frac{c^2-1}{8}} \cdot (-1)^{\frac{p_r^2-1}{8}} = (-1)^{\frac{c^2-1}{8} + \frac{p_r^2-1}{8}} = (-1)^{\frac{b^2-1}{8}}$. Esto concluye la demostración por inducción.

- (c) Aplicamos inducción, pero esta vez la inducción es en n = r + s, donde r es el número de divisores primos (distintos o no) de b y s el de a, es decir:
- $b = p_1 \cdot p_2 \cdot \ldots \cdot p_r$, $a = q_1 \cdot q_2 \cdot \ldots \cdot q_s$ con todos los p_i y los q_j primos.
- La base de la inducción es el caso n=2, que equivale a r=s=1, en este caso a y b son primos y el resultado ya fue probado: es la Ley de Reciprocidad Cuadrática.
- Si n = r+s > 2, supongamos sin pérdida de generalidad que se tiene r >1 (si no fuera así, sería s >1, que se trata análogamente). Sea $c = b/p_r$. Suponemos (hipótesis de inducción) que la propiedad es cierta para n-1 = r+s-1 y también para todo entero menor o igual que n-1 (y mayor o igual que 2), es decir: la propiedad es cierta en el caso en que el total de divisores primos que poseen entre los dos números es w con $2 \leqq w \leqq n-1 = r+s-1$.

- Como este es el caso para el par de números a, c, tenemos: $\left(\frac{a}{c}\right) = \left(\frac{c}{a}\right) \cdot (-1)^{\frac{a-1}{2} \cdot \frac{c-1}{2}}$, que equivale a: $\left(\frac{a}{c}\right) \cdot \left(\frac{c}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{c-1}{2}}$.
- También podemos aplicar la hipótesis de inducción al par de números a, p_r pues en este caso el total de divisores primos es s + 1 ≦ s + r -1 = n-1. Por lo tanto, se tiene: $\left(\frac{a}{p_r}\right) \cdot \left(\frac{p_r}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{p_r-1}{2}}$. Estamos en condiciones de aplicar el lema 3, y obtenemos: $\left(\frac{a}{p_r \cdot c}\right) \cdot \left(\frac{p_r \cdot c}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{p_r \cdot c-1}{2}}$ que, como b = $p_r \cdot c$, es lo que queríamos probar.
- Esto acaba la demostración por inducción.

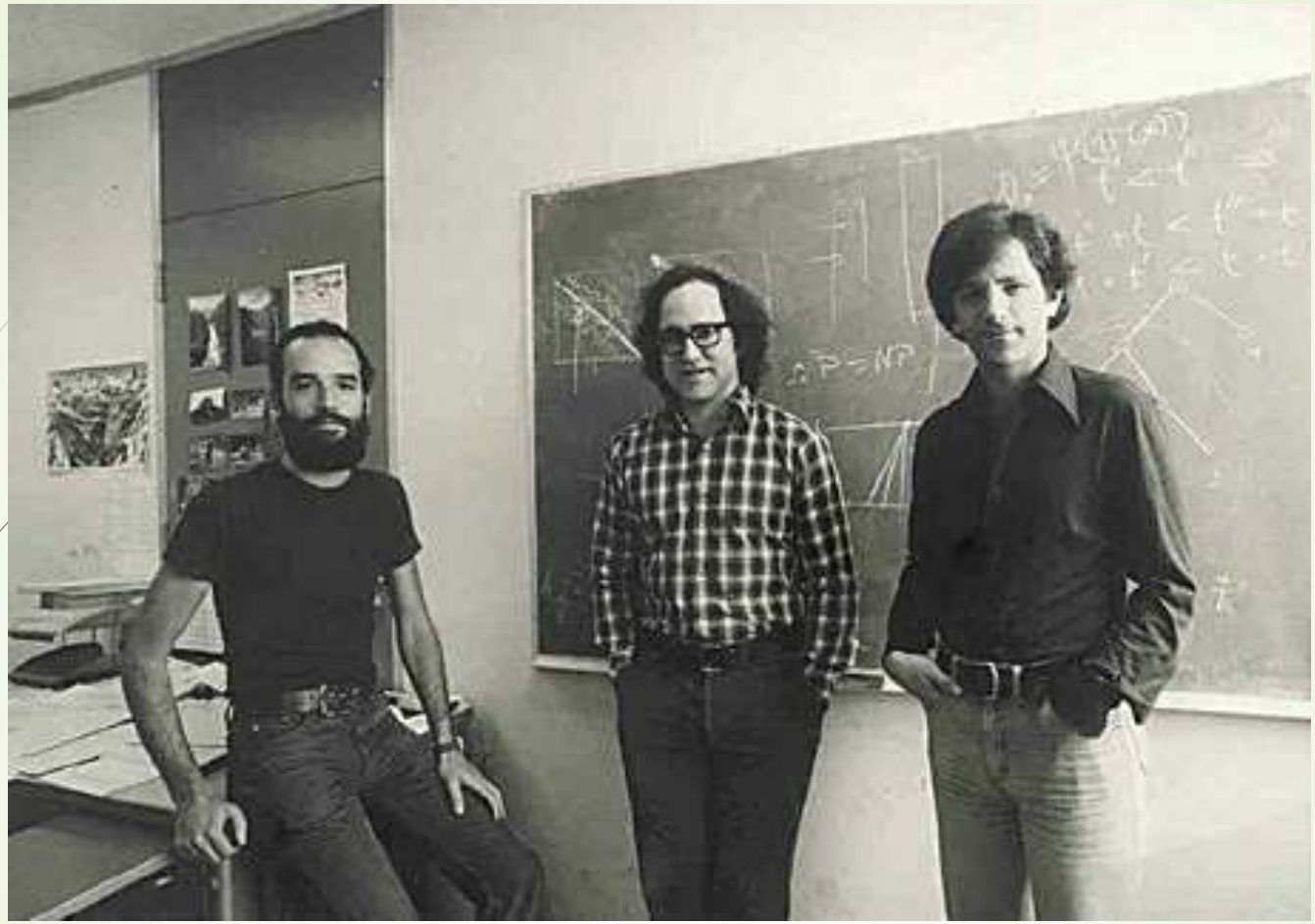
Criptografía de Clave pública: el cirptosistema RSA

- Generalidades:
- La idea que subyace en la criptografía de clave pública es que hay funciones f biyectivas pero tales que dada f no se puede calcular "en la práctica" (al menos, no hay algoritmo eficiente que lo permita) la función inversa de f.
- Por ejemplo, si $S = \mathbb{Z}/n\mathbb{Z}$ para $n = p \cdot q$ con p y q primos grandes (apropiados) veremos que hay funciones $f : S \to S$ biyectivas que aunque se las conozca, y en particular se conozca el valor de n, no se conocen algoritmos que permitan calcular (en un tiempo razonable) su inversa.
- Más precisamente: no se puede determinar la inversa de f EXCEPTO si se factoriza n, y esto hace que el sistema sea seguro pues para p y q suficientemente grandes (y "apropiados") no existen algoritmos rápidos para factorizar $n = p \cdot q$.

- Mediante tales funciones se puede establecer un Criptosistema de Clave Pública: Un usuario, llamémosle Bernat, dispone de una Clave Pública que ES DE DOMINIO PÚBLICO. Identificamos esta clave pública con una función f con las propiedades ya especificadas. Cuando un usuario, llamémosle Alicia, quiere enviar un mensaje $M \in S$ a Bernat, lo encripta utilizando la clave pública $f : S \rightarrow S$ obteniendo $f(M) = X \in S$, el mensaje encriptado.
- Bernat (¡y sólo él!) cuenta con información secreta que hace que sólo él haya podido precalcular la inversa f^{-1} de f: esta es su clave privada, con la cual Bernat desencripta el mensaje encriptado X obteniendo $f^{-1}(X) = M$.
- La principal ventaja es que Bernat y Alica no han tenido que compartir información secreta. Sólo Bernat conoce su clave secreta, no es preciso que Alica la conozca (ella ha utilizado sólo la clave pública de Bernat, que puede estar por ejemplo disponible en su página web).

- En el sistema concreto que veremos es $S = \mathbb{Z}/n\mathbb{Z}$ y el valor de n y de la función f son públicos, donde $n = p \cdot q$ con p y q primos grandes (secretos), y veremos que la única manera (que se conoce) de determinar la inversa de f es conociendo los divisores primos p y q de n, de modo que la seguridad del criptosistema se basa en que no existen algoritmos eficientes para factorizar tales n y hallar p y q.
- ¿Pero entonces, cómo es que Bernat sí los conoce, y los utiliza para desencriptar el mensaje? ¿Es Bernat capaz de factorizar n? No, la cosa es al revés: Bernat COMENZÓ escogiendo p y q y simplemente los multiplicó para construir n, que es el módulo a utilizar para su función f.
- Observación: En la actualidad, se está cada vez más cerca de construir un nuevo tipo de ordenadores, llamados ORDENADORES CUÁNTICOS. En cuanto estos estén disponibles, este criptosistema dejará de ser seguro pues ya se dispone de algoritmos (cuánticos) eficientes para factorizar enteros $n = p \cdot q$ con estos ordenadores.

Clase 22



- Shamir Rivest Adleman

- El Criptosistema RSA:
- Para construir la clave pública y la clave privada, Bernat comienza escogiendo dos primos muy grandes p y q y calcula su producto n. Estos dos primos deben ser escogidos con cuidado pues hay casos especiales en los que, a pesar de tener ambos primos un tamaño apropiado (el tamaño depende de los estándares del momento), se puede factorizar de manera eficiente $n = p \cdot q$. Más adelante en este curso veremos algunos de estos algoritmos. Por lo tanto, Bernat se asegurará de evitar estos casos para que la factorización de n no sea practicable.
- Observemos que si $n = p \cdot q$, se tiene que la función φ de Euler comple: $\varphi(n) = (p-1)\cdot(q-1)$. Por lo tanto, si se conocen los divisores primos p y q de n, es sencillo calcular $\varphi(n)$. Recíprocamente, si se conoce $\varphi(n)$, como este valor es igual a $(p-1)\cdot(q-1)$ ya se tiene dos ecuaciones que satisfacen los primos p y q:

- $p \cdot q = n$, y $(p-1)\cdot(q-1) = \varphi(n)$.
- Es fácil resolver este sistema de dos ecuaciones con dos incógnitas (aun que no sea lineal: por sustitución se reduce a resolver una ecuación cuadrática) y por lo tanto determinar p y q si se conocen n y $\varphi(n)$.
- Esto prueba que factorizar n y determinar en valor de $\varphi(n)$ son problemas equivalentes. Esta observación es importante pues la seguridad del criptosistema depende precisamente del hecho de que nadie que no conozca la clave privada pueda calcular $\varphi(n)$.
- Una vez escogido el módulo n con el que trabajar, Bernat tiene que escoger la función biyectiva $f: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ con la que encriptar. En el RSA, esta función será de la siguiente forma: Bernat escoge un entero positivo e, el "exponente", no demasiado pequeño, que será su clave pública y la función f asociada a este e es:
- $$f(a) \equiv a^e \pmod{n}$$
- Podemos coger como conjunto de mensajes representantes en el intervalo [1,n] de las clases residuales módulo n, y el mensaje encriptado también será un entero en este intervalo.

- Veamos cual es la función inversa de f. Antes de seguir, supondremos que el mensaje a, que es el elemento de $\mathbb{Z}/n\mathbb{Z}$ al que se aplica f, es una clase inversible módulo n, es decir, es coprimo con n. En la práctica esto ocurre con una probabilidad tan alta que podemos suponer que siempre será así (pues esta condición equivale a pedir que p ł a y q ł a).
- Luego, tenemos:
- f: $(\mathbb{Z}/n\mathbb{Z})^* \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ con: $f(a) = a^e \pmod n$.
- La clave privada, que sólo Bernat conoce, consiste en un elemento d tal que: $e \cdot d \equiv 1 \pmod{\varphi(n)}$.
- Antes de ver como se utiliza este d para desencriptar un mensaje, analicemos la seguridad del sistema. Por un lado, Bernat, que conoce p y q, puede calcular sencillamente $\varphi(n) = (p-1)\cdot(q-1)$, y luego calcular d, que es el inverso de e módulo $\varphi(n)$, utilizando el Algoritmo de Euclides extendido (que resuelve la identidad de Bézout) como ya vimos en este curso. Un detalle técnico: hace falta imponer que e sea coprimo con $\varphi(n)$, por lo tanto Bernat tiene que tener en cuenta esta condición al escoger e.

- Cualquier otra persona, que sólo dispone de la información pública, es decir, de n y de e, no conoce los divisores primos p y q de n (ni puede calcularlos), y como ya comentamos antes, esto hace que sea imposible para esta persona calcular φ(n). Como ni siquiera conoce φ(n), le es imposible determinar d, pues para hacerlo tendría que calcular el inverso de e en un módulo que le es desconocido!
- Veamos ahora como con su clave secreta d Bernat puede desencriptar los mensajes que recibe. El procedimiento es similar al de encriptado, sólo que en lugar de elevar a la e ahora hay que elevar a la d. Que esto da la función inversa buscada lo prueba el siguiente resultado.

- Lema: Si f: $(\mathbb{Z}/n\mathbb{Z})^* \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ viene dada por la ley: $f(a) \equiv a^e \pmod n$, para un e > 1 inversible módulo $\varphi(n)$, y d > 0 cumple: $e \cdot d \equiv 1 \pmod{\varphi(n)}$, entonces la inversa f^{-1} de f viene dada por: $f^{-1}(z) \equiv z^d \pmod n$.
- Demostración: Tenemos que probar que la composición de estas dos funciones (en cualquier orden) es la identidad en $(\mathbb{Z}/n\mathbb{Z})^*$, es decir, que para todo a inversible módulo n, vale: $(a^e)^d \equiv a \pmod n$ y $(a^d)^e \equiv a \pmod n$. Ambas equivalen a : $a^{e\cdot d} \equiv a \pmod n$.
- Como $e \cdot d \equiv 1 \pmod{\varphi(n)} \Rightarrow e \cdot d = k \cdot \varphi(n) + 1$, para un $k \in \mathbb{Z}$, $k \geqq 1$.
- Como a es inversible módulo n, por el Teorema de Euler:
- $a^{\varphi(n)} \equiv 1 \pmod n \Rightarrow a^{e\cdot d} \equiv a^{k\cdot\varphi(n)+1} \equiv (a^{\varphi(n)})^k \cdot a \equiv 1 \cdot a \equiv a \pmod n$.
- Esto prueba que elevar a la d módulo n es la función inversa de f.

- Por lo tanto, dado un mensaje $M \in (\mathbb{Z}/n\mathbb{Z})^*$ que Alicia quiere enviar a Bernat, haciendo uso de la clave pública (n,e) de Bernat, Alicia calcula:
- $f(M) \equiv M^e \equiv X \pmod{n}$ que es el mensaje encriptado que se envía.
- Bernat, que conoce la información secreta (p, q , $\varphi(n)$) donde $n = p \cdot q$ y a través de ellos ha calculado la clave secreta d definida como en el lema previo, la utiliza para desencriptar calculando: $X^d \equiv f^{-1}(X) \equiv M \pmod{n}$.
- En principio (si bien en la práctica otros ataques son posibles) no se puede desencriptar un mensaje encriptado a pesar de que se conoce la clave pública (n,e) puesto que no se sabe como factorizar n (en un tiempo razonable) y por lo tanto no se puede calcular $\varphi(n)$, de modo que no se puede determinar el valor de d necesario para desencriptar.