http://www.thenaturalamerican.com/wind_talker_dictionary.htm

The Navajo Code Talkers

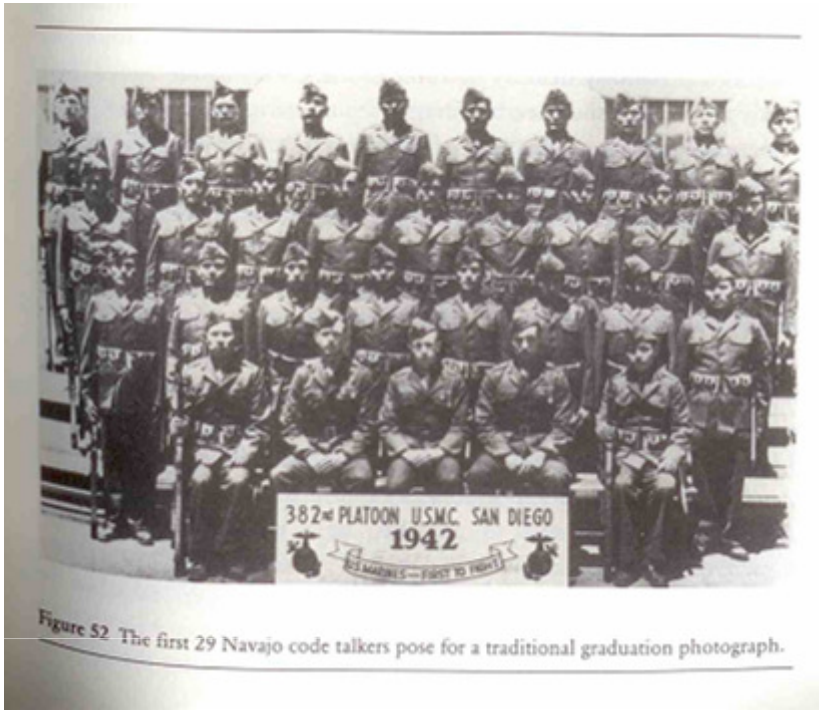


Figure 52 The first 29 Navajo code talkers pose for a traditional graduation photograph.

Table 12 The Navajo alphabet code.

A	Ant	Wol-la-chee	N	Nut	Nesh-chee
B	Bear	Shush	O	Owl	Ne-ahs-jsh
C	Cat	Moasi	P	Pig	Bi-sodih
D	Deer	Be	Q	Quiver	Ca-yeilth
E	Elk	Dzeh	R	Rabbit	Gah
F	Fox	Ma-e	S	Sheep	Dibeh
G	Goat	Klizzie	T	Turkey	Than-zie
H	Horse	Lin	U	Ute	No-da-ih
I	Ice	Tkin	V	Victor	A-keh-di-glini
J	Jackass	Tkele-cho-gi	W	Weasel	Gloe-ih
K	Kid	Klizzie-yazzi	X	Cross	Al-an-as-dzoh
L	Lamb	Dibeh-yazzi	Y	Yucca	Tsah-as-zih
M	Mouse	Na-as-tso-si	Z	Zinc	Besh-do-gliz

Table 11 Navajo codewords for planes and ships.

Fighter plane	Hummingbird	Da-he-tih-hi
Observation plane	Owl	Ne-as-jah
Torpedo plane	Swallow	Tas-chizzie
Bomber	Buzzard	Jay-sho
Dive-bomber	Chicken hawk	Gini
Bombs	Eggs	A-ye-shi
Amphibious vehicle	Frog	Chal
Battleship	Whale	Lo-tso
Destroyer	Shark	Ca-lo
Submarine		

Figure 53 Corporal Henry Bake, Jr. (left) and Private First Class George H. Kirk using the Navajo code in the dense jungles of Bougainville in 1943.

Pictures from "The Code Book", by Simon Singh, 1999

The Navajo Code Talkers (II Guerra Mundial, 1939 - 1945**)**

• Mientras los británicos rompían Enigma (Alemania), los norteamericanos luchaban en el pacífico contra los japoneses. Su arma secreta eran los indios navajos.

• Philip Johnston (1892-1978, ingeniero). De niño vivió en reserva india. Contó la idea de usar el navajo para codificar los mensajes en la guerra.

• El navajo es una lengua hablada, no escrita. Ninguna otra tribu los entiende. Solo 28 americanos la conocían.

• Los navajos se entrenaron y crearon palabras código para la guerra:
    • Avión = búho = da-he-tih-hi
    • Bomba = huevo = a-ye-shi
    • barco = ballena = lo-tso
    • destructor = tiburón = ca-lo
    • tanque = tortuga = chay-da-gahi
• Además, crearon un alfabeto: A = ANT = wol-la-chee
• Tardaban 4 minutos en codificar/emitir radio/descodificar mientras que antes tardaban horas.
• Los navajos pasaron de ser ciudadanos de segunda a héroes. Les mimaban y protegían. Pero también les mataban si era necesario.
• En Iwo Jima enviaron más de 800 mensajes. Los japoneses nunca los descifraron.
• Tras la guerra todo se mantuvo Top Secret, hasta 1982 cuando se les rindió homenaje.
• Filmografía:
    • *Wind talkers*, 2002, con Nicolas Cage
    •*Flags of our fathers* (EEUU), *Lamps before the wind* (Japón), 2006, Clint Eastwood.

The Code Book, by Simon Singh

Figure 38 Arthur Scherbius.

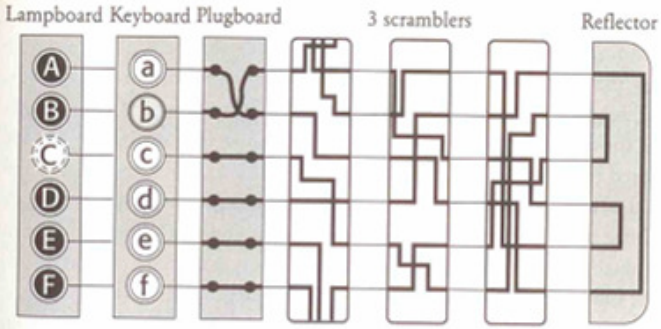


Figure 37 The plugboard sits between the keyboard and the first scrambler. By inserting cables it is possible to swap pairs of letters, so that, in this case, b is swapped with a. Now, b is encrypted by following the path previously associated with the encryption of a. In the real 26-letter Enigma, the user would have six cables for swapping six pairs of letters.

Máquina de cifrar Enigma

dispositivo electromecánico
cifrado rotatorio
patente 1919
usado Alemania desde 1930

Figure 43 General Heinz Guderian's command post vehicle. An Enigma machine can be seen in use in the bottom left.

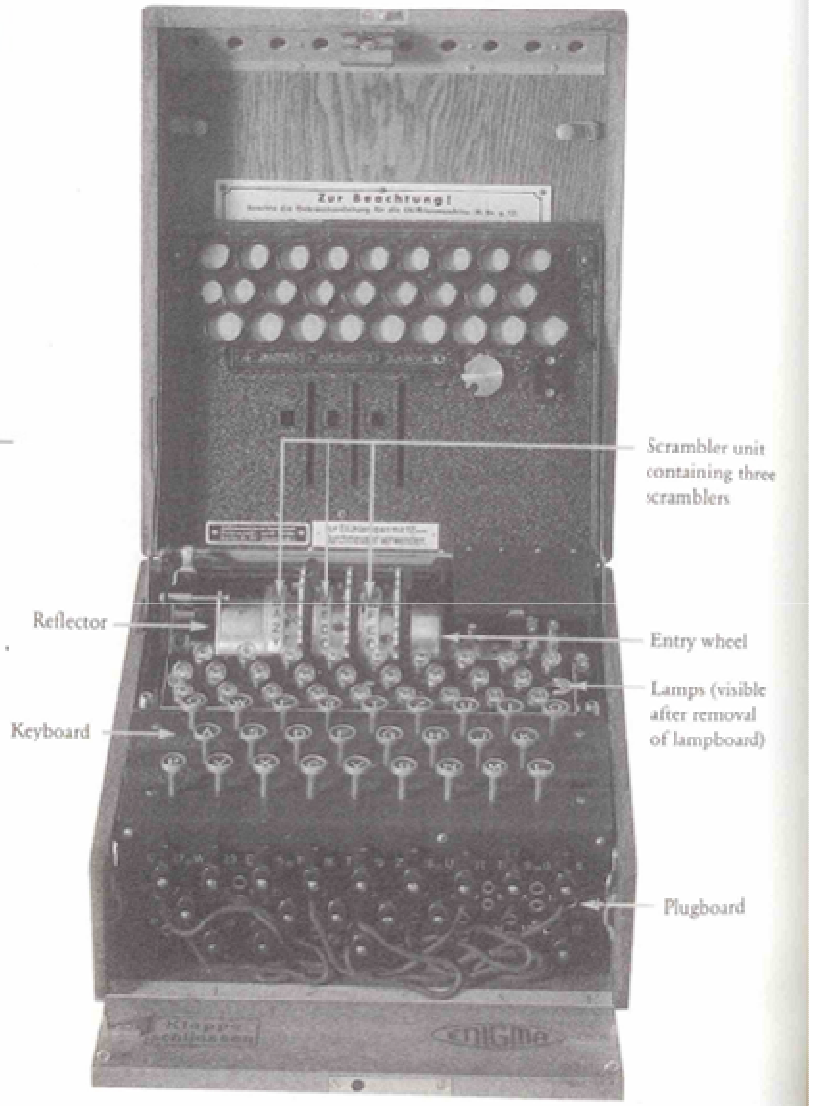


Figure 40 An Enigma machine with the inner lid opened, revealing the three scramblers.

Bletchley Park: Reunieron a matemáticos y criptógrafos británicos, jugadores de ajedrez y bridge y fanáticos de los crucigramas. Los criptoanalistas tenían que romper ENIGMA.

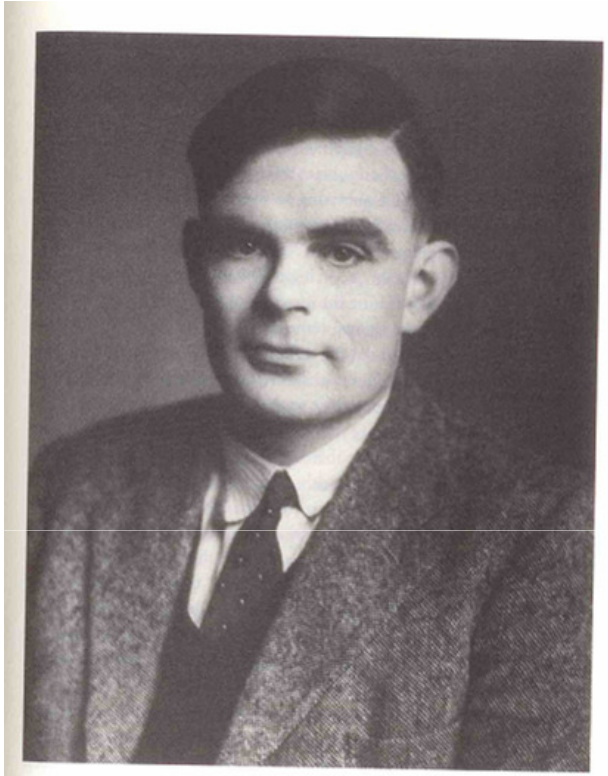


Figure 47 Alan Turing.

Alan Turing (1912, Londres – 1954, Cheshire) matemático, informático teórico, criptógrafo y filósofo inglés.
http://mitworld.mit.edu/video/423

Uno de los padres de la ciencia de la computación, precursor de la informática moderna.
Director sección Naval Enigma del Bletchley Park.
Se estima que contribuyó a acortar la Guerra en dos años.
Diseñó el primer computador electrónico programables digital.

Figure 44 In August 1939, Britain's senior codebreakers visited Bletchley Park to assess its suitability as the site for the new Government Code and Cypher School. To avoid arousing suspicion from locals, they claimed to be part of Captain Ridley's shooting party.

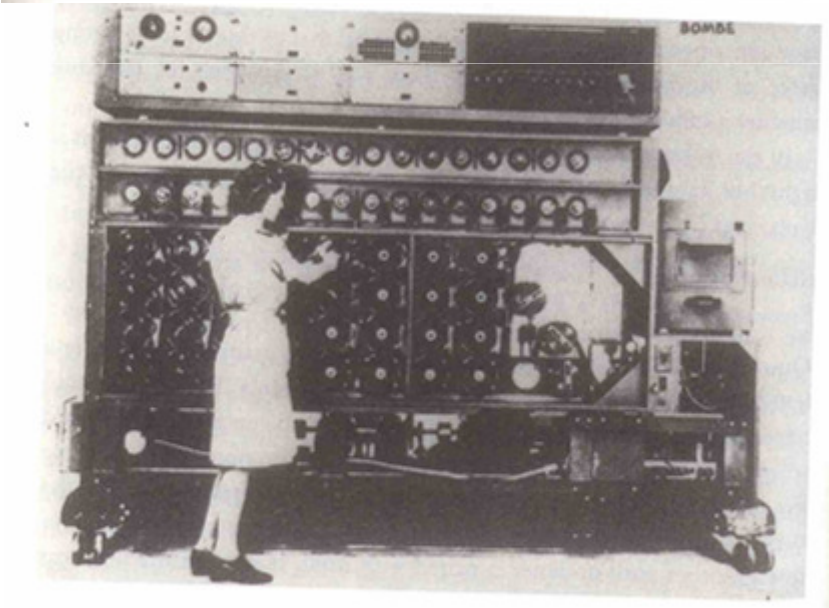
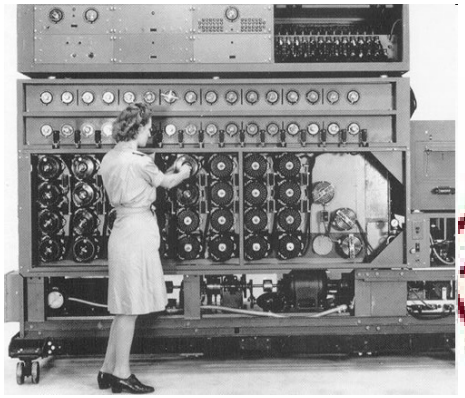


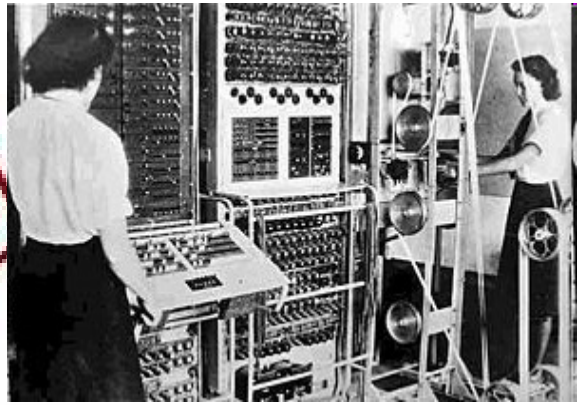
Figure 50 A bombe in action.

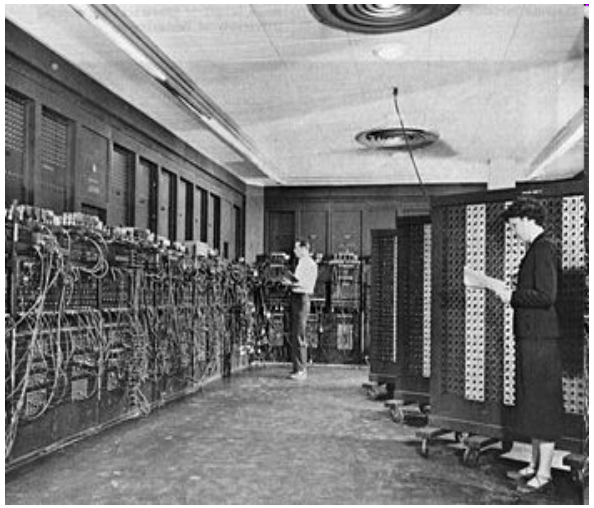
"Las chicas Dilly", resolvieron muchos criptogramas alemanes

The Code Book, Simon Singh



<1970s





Bomba de Turing, Bletchley Park, **1940** (Alan Turing) criptoanálisis ENIGMA, 1ª máquina electromecánica programable.

Colossus, Bletchley Park, **1944** (Newman, Flowers), criptoanálisis ENIGMA, 2000 válvulas electrónicas. 1ª máquina digital programable.

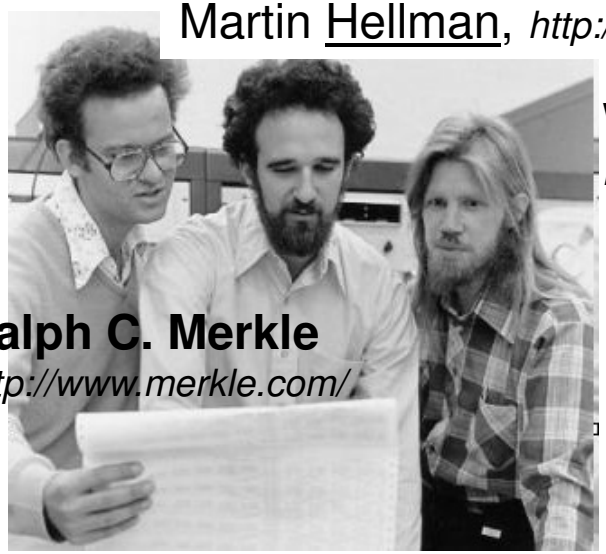
ENIAC (Electronic Numerical Integrator And Computer), University of Pensilvania, **1945** (Eckert, Mauchly), 18000 válvulas electrónicas, 5000 sumas/seg. Considerada la Madre de las Computadoras, hasta los 70s. (170m^2, 27Tm)

1973, NSA (*National Security Agency*) busca algoritmo de cifrado seguro: Lucifer (Horst Feistel, emigrante alemán controlado por la NSA hasta que entra en IBM y puede trabajar tranquilo en criptografía) evoluciona al DES (*Data Encryption Standard*) y lo estandariza en 1976. Los negocios ya pueden comunicarse de modo seguro.

Problema: Distribución de claves (*hombre del maletín* reparte claves semanalmente!)

1969, nace ARPAnet (4 ordenadores). En **1982**, se extiende a Internet. Hoy hay unos mil millones de ordenadores en el mundo.

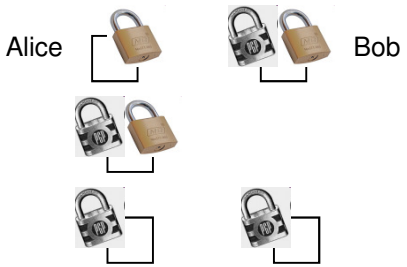
Martin Hellman, *http://www-ee.stanford.edu/~hellman/*



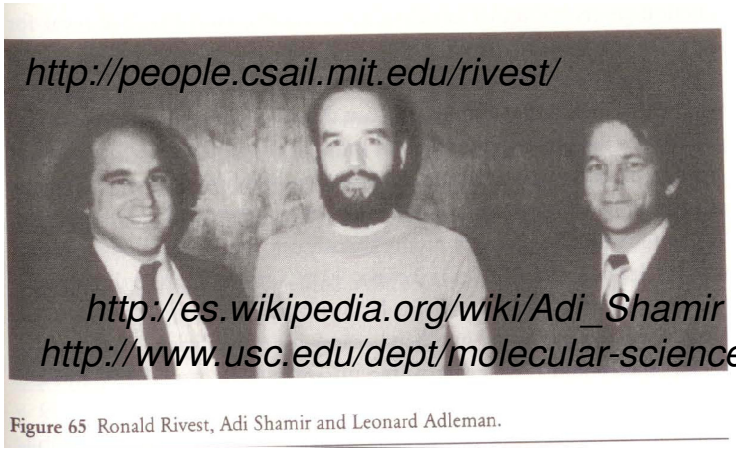
Ralph C. Merkle
http://www.merkle.com/

Whitfield Diffie,
http://research.sun.com/people/diffie/

Key exchange scheme



1976, **Protocolo Diffie-Hellman-Merkle** para intercambio clave secreta de forma remota.
Problema: hasta que no intercambian ambos la clave, no pueden cifrar. Diffie empezó a pensar en Criptografía Asimétrica, pero necesitaba una *función de sentido único*…



http://people.csail.mit.edu/rivest/

http://es.wikipedia.org/wiki/Adi_Shamir
http://www.usc.edu/dept/molecular-science/fm-adleman.htm

Figure 65 Ronald Rivest, Adi Shamir and Leonard Adleman.

RSA, N≈10^{308}, 100 millones de PC tardarían1000 años en romperlo

Public Key Cryptography

1977, Ronald Rivest, Adi Shamir, Leonard Adleman. Trabajan 1 año. Rivest halla la función difícil.
Algoritmo RSA, *http://www.rsa.com/* Patente caducó en 21/09/2000

1982, le visita.

British Government Communications Headquarters, *http://www.gchq.gov.uk/*

1976, Protocolo Diffie-Hellman-Merkle

Key exchange scheme

James Ellis, matemático e informático. En **1969** inventa el concepto de **Public Key Cryptography** (PKC).
Es información clasificada por la GCHG hasta los 90s.
Le faltaba la función difícil…

Figure 66 James Ellis.

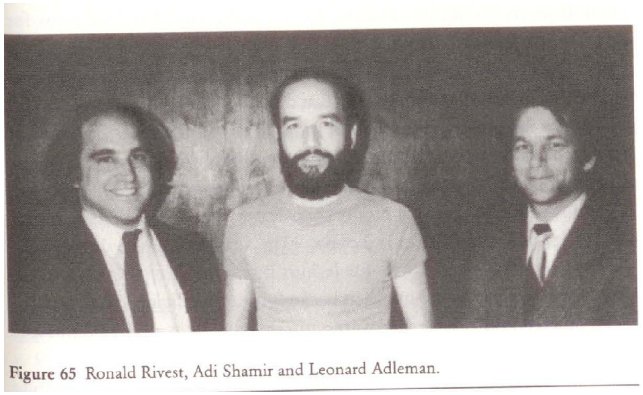


Figure 65 Ronald Rivest, Adi Shamir and Leonard Adleman.

1977, Rivest, Shamir, Adleman

Public Key Cryptography

http://www.rsa.com/
Desarrollan RSA comercialmente. Hoy es la base de toda transacción segura en Internet.

Clifford Cocks, entra en GCHG en **1973**, recién graduado en matemáticas en Cambridge. Le comentan la idea de Ellis. En 30 minutos lo tenía resuelto.

Malcolm J. Williamson, **1974**, GCHQ, diseña el mismo protocolo *Diffie-Hellman-Merkle*.

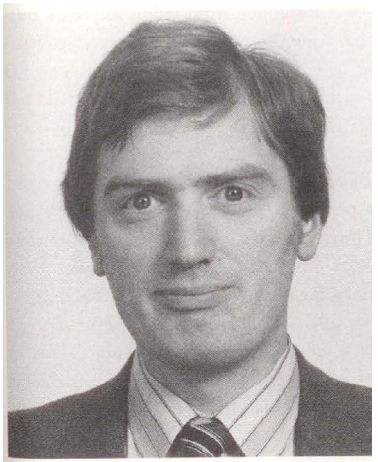


Figure 67 Clifford Cocks.

Cocks da charla en diciembre 1997 y lo cuenta todo, autorizado. Ellis murió 1 mes antes.

PGP (*Pretty Good Privacy*), Phil Zimmermann, *http://www.philzimmermann.com*

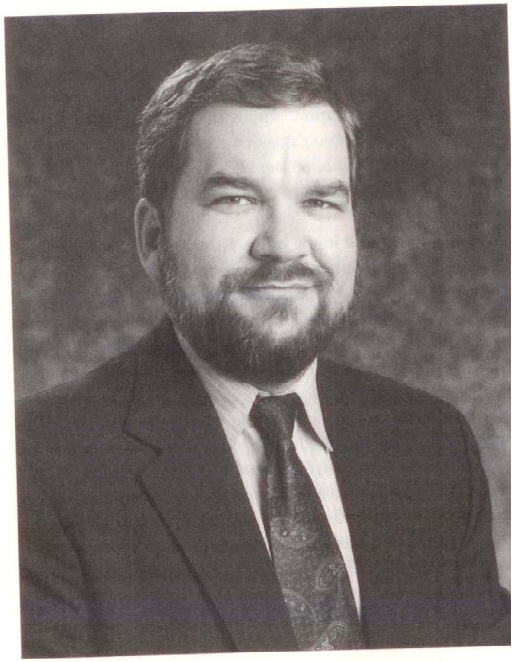


Figure 70 Phil Zimmermann.

Software de cifrado, firma y autenticación, sencillo de utilizar por el público en general.

1980s, Contra las armas nucleares, a favor del derecho a la comunicación segura civil → El FBI le investiga.

En los 80 solo usaban RSA el Gobierno, los militares y las grandes compañías, que tenían grandes ordenadores.

Phil desarrolla una plataforma sencilla para extender su uso en la población. Cómo autenticar claves con RSA, cómo cifrar con DES. Espera una licencia RSA para comercializar su producto.

Voto electrónico,
Telefonía digital segura…

En 1991, el Senado pretende endurecer la ley de exportación de *software* de cifrado de Estados Unidos!!

Phil cuelga PGP del servidor de un amigo. Pronto activistas, pacifistas… de todo el mundo lo usan. Pero también terroristas… En 1993, el FBI le investiga por 3 años, pero al final lo dejan sin cargos. RSA le deja la licencia. El MIT le avala. *http://pgpi.com*