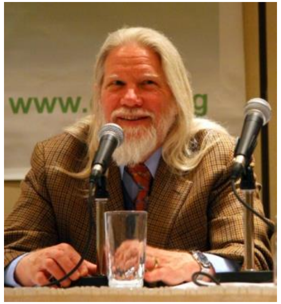
The RSA Cryptosystems (1)

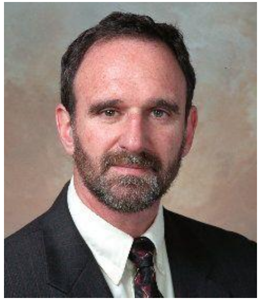
- **Prime numbers** and **cryptosystems** have been studied for 2000 years.
- The usefulness of prime numbers to cryptography was noticed only in 1970’s.
- In 1976, Diffie and Hellman published the notion of **Public Key Cryptography** using **asymmetric** **(non-symmetric)** encryption/decryption keys.

The RSA Cryptosystems (2)

- Diffie and Hellman published a method to share a secret key using **exponentiation (mod P)**. (**Diffie-Hellman Key Exchange**)
- But they could not find a method to encrypt messages.



Bailey Whitfield Diffie
(1944-)



Martin Edward Hellman
(1945-)

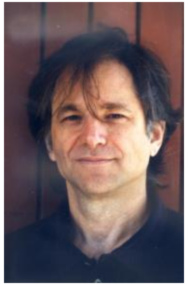
https://en.wikipedia.org/wiki/Whitfield_Diffie
https://en.wikipedia.org/wiki/Martin_Hellman

The RSA Cryptosystems (3)

- In 1978, Rivest, Shamir, and Adleman invented the first practical public key encryption system (**RSA**).
- They used **exponentiation (mod N)**, where N=PQ is a product of **two large prime numbers**.

Ronald Linn Rivest (1947-)

Adi Shamir (1952-)



Leonard Adleman (1945-)

https://en.wikipedia.org/wiki/Ron_Rivest
https://en.wikipedia.org/wiki/Adi_Shamir
https://en.wikipedia.org/wiki/Leonard_Adleman

The RSA Cryptosystems (4)

- RSA is a practical cryptosystems.
  It is still widely used.
- Today, many public key cryptosystems using prime numbers were invented.

The RSA Cryptosystems (5)

- In 1985, Elgamal invented a public key encryption system based on Diffie-Hellman's ideas. (**ElGamal Encryption System**)
- Elgamal used **exponentiation (mod P)**, and **Primitive Roots of Unity (mod P).** Elgamal's method was further generalized to design **Elliptic Curve Cryptosystems**.

Taher Elgamal
(1955-)

https://en.wikipedia.org/wiki/Taher_Elgamal