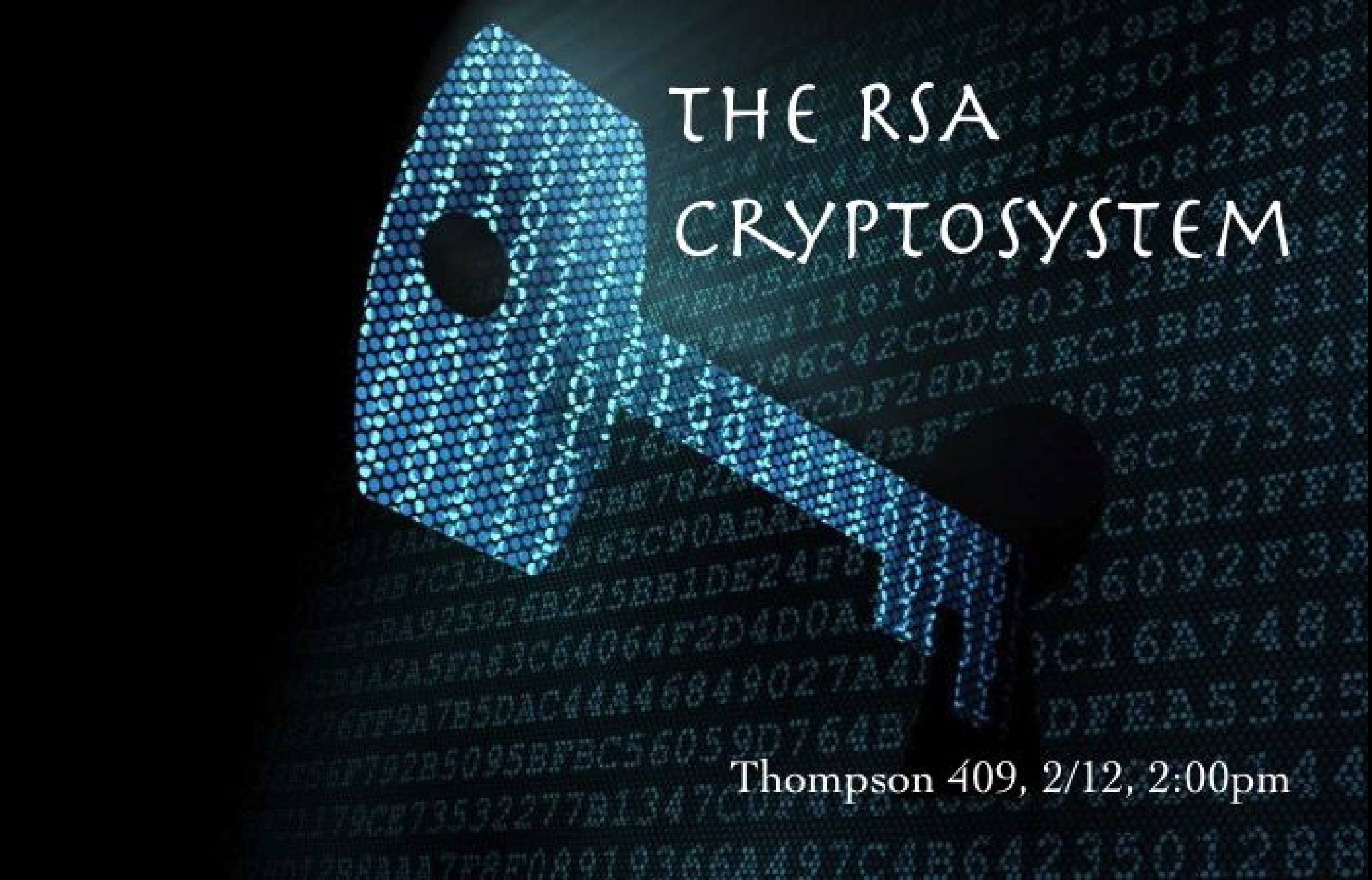

THE RSA
CRYPTOSYSTEM
Thompson 409, 2/12, 2:00pm

What is RSA for?

Suppose you're using a web page (Amazon) and need to send some confidential information (your credit card number, etc.).

Problem: Internet communication is very insecure. (Someone untrustworthy could be listening!)

Solution: *encrypt* the information using a public key so that only permitted entities (Amazon) can *decrypt* it.

This is the basis of *public-key cryptography*.

But how do we do this?

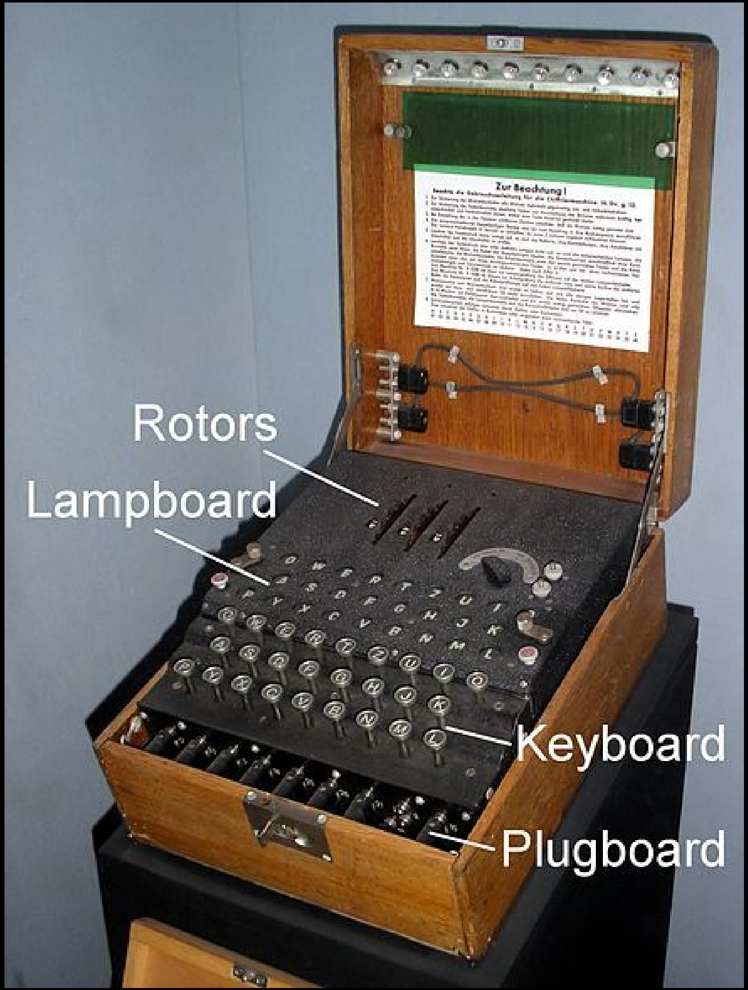
Historical Progression

Earliest: Egypt, 1900 BC

Private key: Caesar cipher

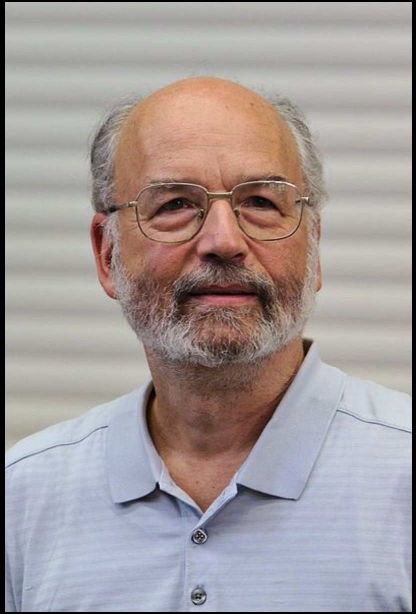
Post-WWI to WWII: Enigma cipher

Going public: Diffie-Hellman key exchange (1976)

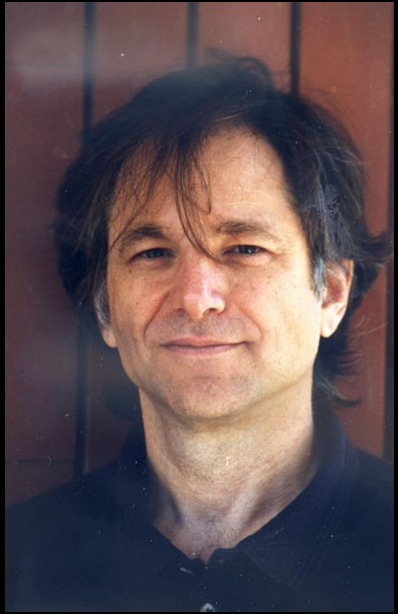


Enter RSA (1977)

Ronald R. **R**ivest



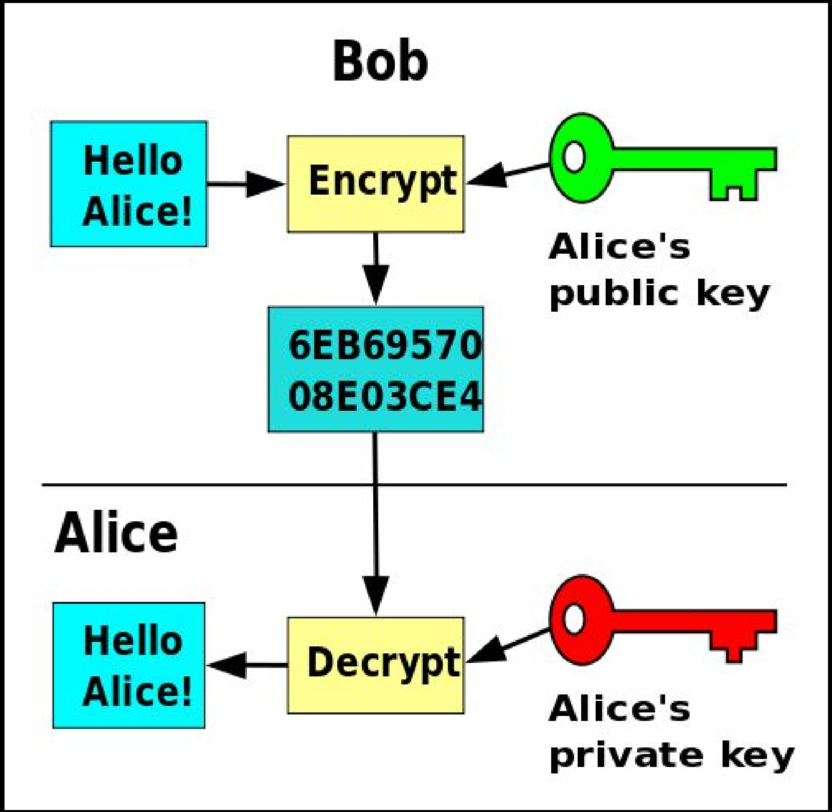
Adi **S**hamir



Leonard **A**dleman

Public Key Cryptography

Bob talks to Alice:



The RSA cryptosystem procedure

Pick two prime numbers p and q and let

$n = pq$, $m = \phi(n) = (p-1)(q-1)$.

Pick a positive integer E such that $\gcd(m, E) = 1$.

Find D such that $DE \bmod m = 1$.

Publish n and E.

Sender: Encode a message M: $M' = M^E \bmod n$.

Receiver: Decode M': $M = M'^D \bmod n$.

Example

Bob sends a message $M = 25$. Alice's key is $n = pq = (23)(29) = 667$.

$m = \phi(n) = 616$; $E = 487$ since $\gcd(616, 487) = 1$.

Bob encodes his message with n and E: $M' = 25^{487} \bmod 667 = 169$.

Alice uses $D = 191$ (since $DE \bmod n = (191)(487) \bmod 616 = 1$) to decrypt Bob's message:

$M = 169^{191} \bmod 667 = 25$.

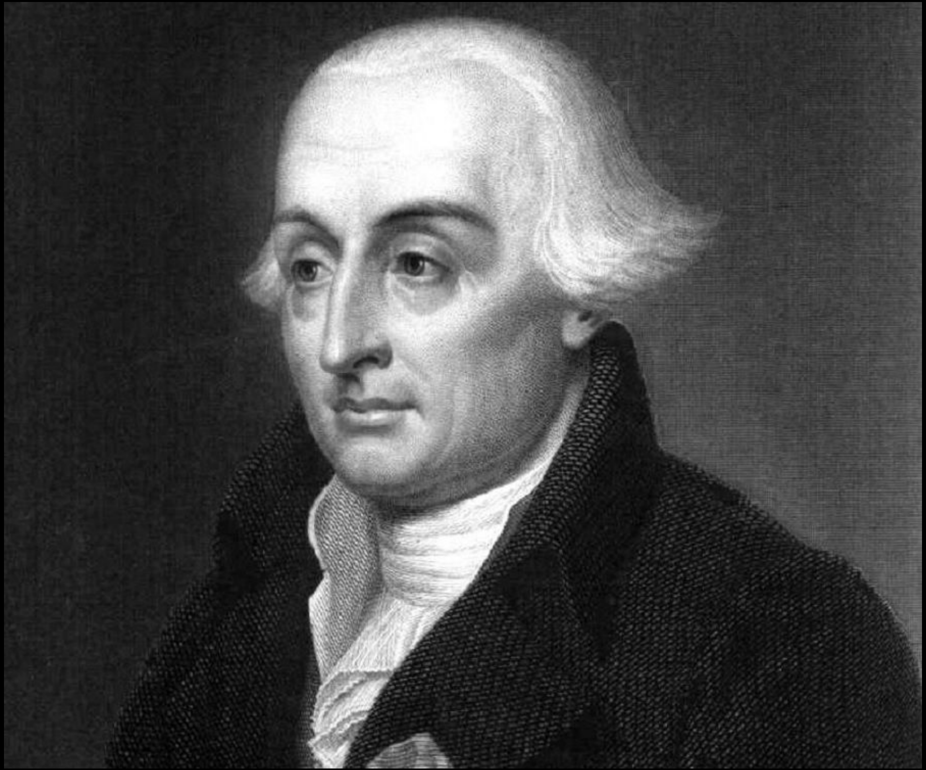
You can check these computations yourself, and create your own keys!

Why we can use RSA

Multiply two large primes: easy

Factor the product of two large primes: computationally prohibitive

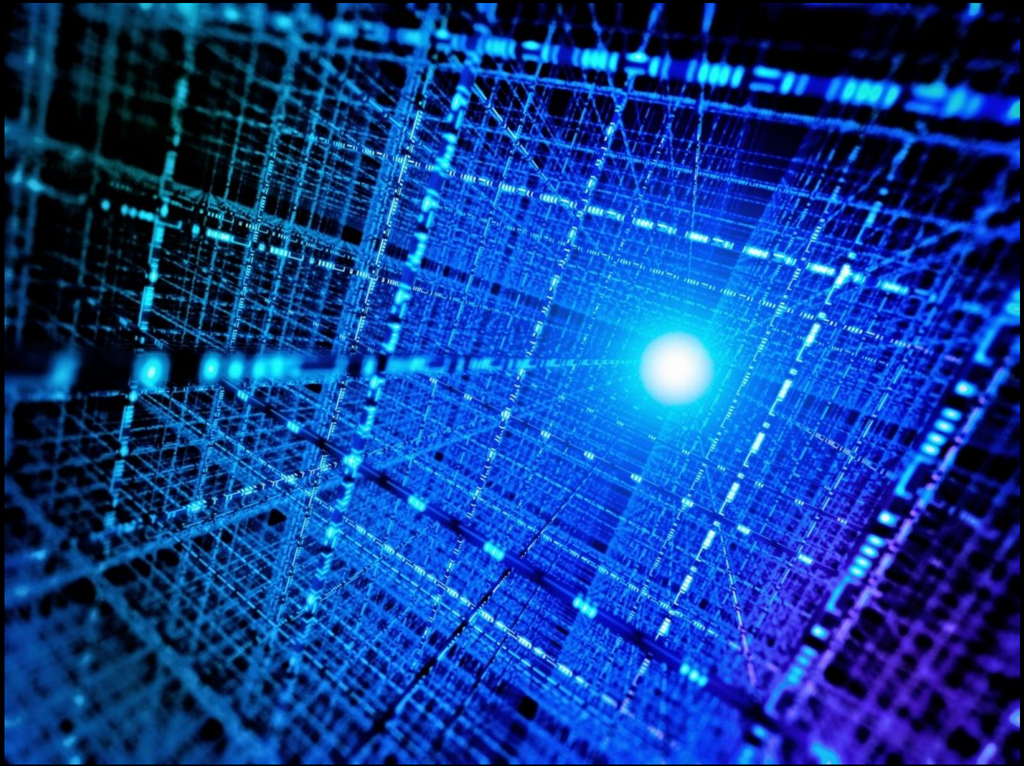
To prove that our message can always be retrieved, we need a result from Abstract Algebra (Lagrange's Theorem from group theory)



Future of RSA

Uncertain.

According to *Shor's Algorithm*, a quantum computer could factor any large integer in polynomial time.



Further crypto

Source: T. Judson, *Abstract Algebra: Theory and Applications* (examples from 7.2)

Simon Singh, *The Code Book*

Neal Stephenson, *Cryptonomicon*

Abstract Algebra I (MATH 433, fall semester. Prerequisite: Linear Algebra)

Study abroad in Budapest program