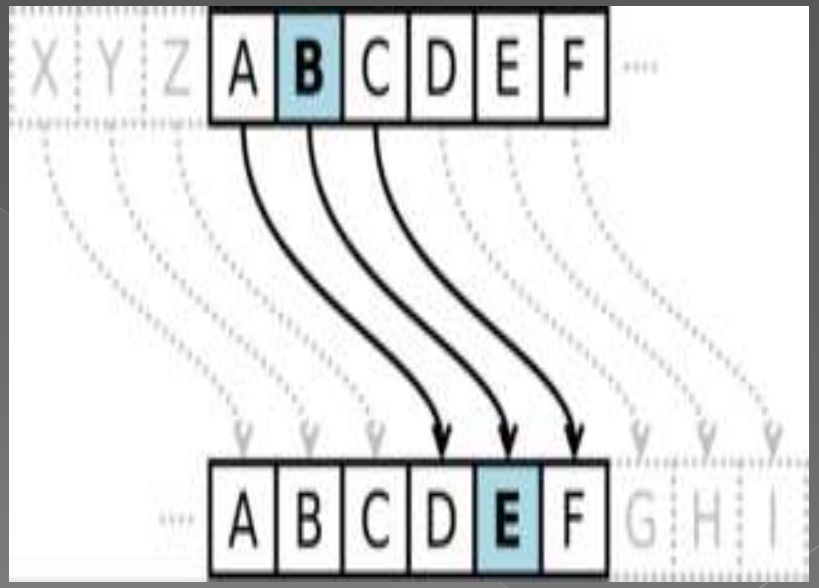
RSA Encryption

Shannon Keenan

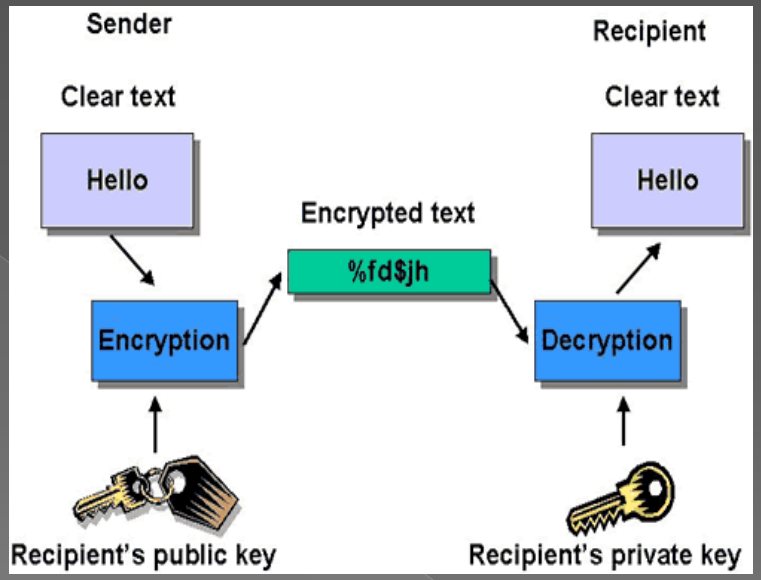
Cryptography

- Study of hidden messages
- http://www.youtube.com/watch?v=H5OWoG44VAw
- Pig Latin
- Caesar cipher
- All two-way ciphers



Trap Door Cipher

- Coding is one-way
- Easy to encode, difficult to decode
- Only Alice knows how to decode her message
- Safest way to send a message, keep from hackers



RSA Encryption

- Trap-door cipher
- Factoring Problem
- Semiprime numbers

RSA Encryption

- Encoding key: $C=M^e \bmod N$ (N,e)
- Decoding key: $M=C^d \bmod N$ (N,d)
- $N=pq$
- $\varphi=(p-1)(q-1)$
- e is coprime to φ
- d is the modular multiplicative inverse to $e \bmod \varphi$.
- $ed=1 \bmod \varphi$
- ed-1 divides φ

Jenna wants to send Dan a Message

- Dan chooses p=11, q=5
- N=55, φ=(11-1)(5-1)=40
- e=3
- ed=1modφ
  Extended Euclidian algorithm:
  ed-1=φa
  3d-1=40a
  d=(1+40a)/3
  a=2,**d=27**

- Public key: (N,e) to Jenna: (55,3)
- Private key: (N,d)=(55,27)
- Jenna Uses encoding key $C=M^e \mod N$
- $C=7^3 \mod 55$
- C=13

Dan Decodes Jenna's Message

- Dan receives the message "13"
- Decoding key: $M=C^d \text{mod} N$
- $M=13^{27} \text{mod} 55$
- $13^{27}=13^{16}*13^{8}*13^{2}*13^{1}$
- Property of modular arithmetic: $bc \text{mod} n=(b \text{mod} n * c \text{mod} n) \text{mod} n$
- Compute partial modulus in a table:

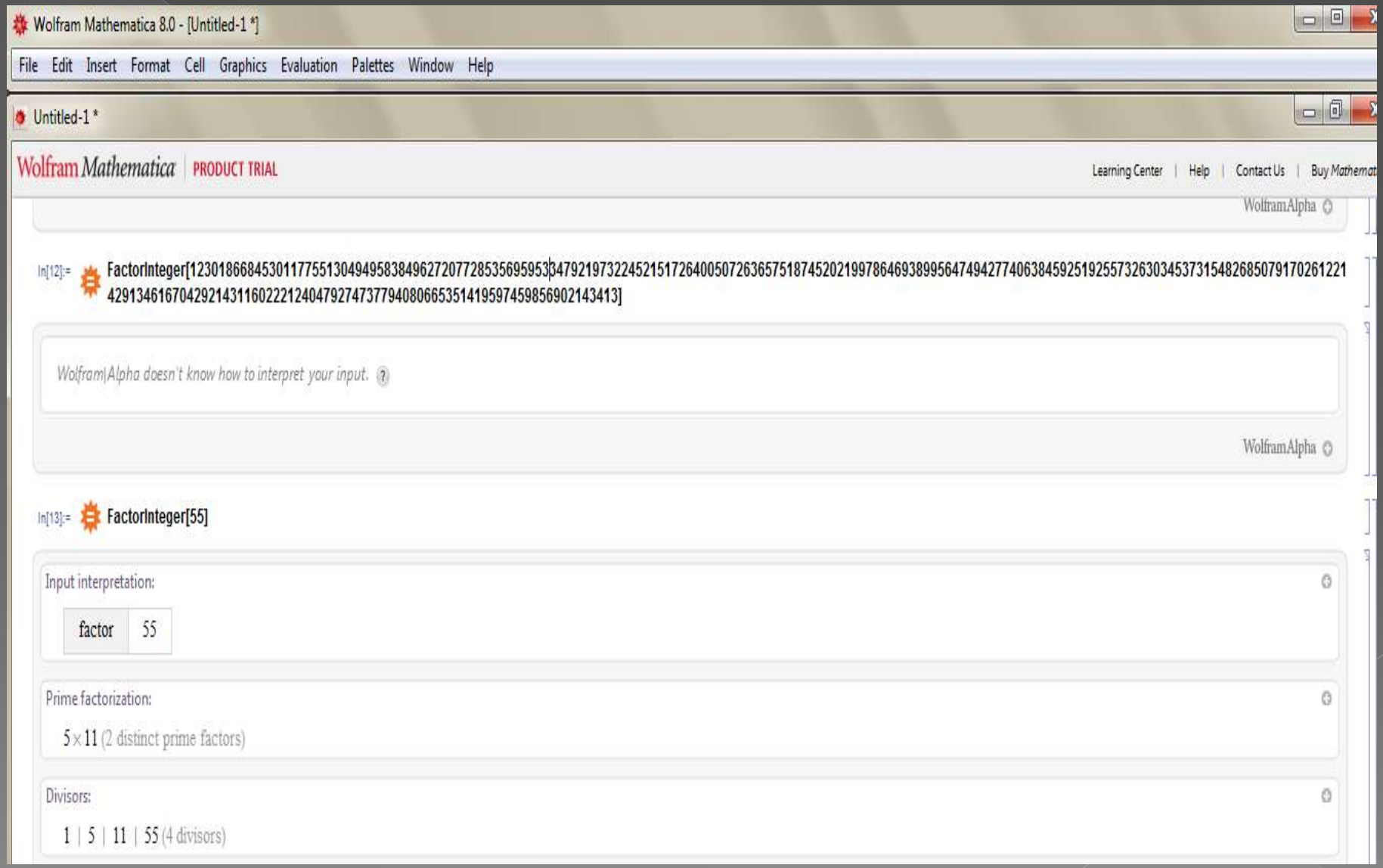
- $13^1 \text{mod} 55=13$
  $13^2 \text{mod} 55=4$
  $(13^2)^2 \text{mod} 55=16$
  $(13^4)^2 \text{mod} 55=36$
  $(13^8)^2 \text{mod} 55=31$
- $(13*4*36*31) \text{mod} 55=7$

Chinese Remainder Theorem

- Calculate d_p,d_q ,q^{-1}, and h
- d_p= dmod(p-1)
- d_p=27mod10 **d_p=7**
- d_q=dmod(q-1)
- d_q=27mod4, **d_q= 3**
- q^{-1}= $d_q$modp,
- q^{-1}=3mod11, **q^{-1}=3**
- m_1=c^{dp}modp
- m_1=13^7mod11, **m_1=7**
- m_2=c^{dq}modq
- m_2=13^3mod5, **m_2=3**
- h=(q^{-1}*(m_1-m_2))modp
- h=(3*(7-3))mod11
- h=12mod11, **h=1**
- **M=m_2+h*q**
- M=3+1*4, **M=7**
- More efficient way of decoding

Very Secure! Using large N

- Factoring problem
- Trap door
- Computers cannot factor large integers
- Trusted by billions


Wolfram Mathematica 8.0 - [Untitled-1 *]
File Edit Insert Format Cell Graphics Evaluation Palettes Window Help
Untitled-1 *
Wolfram Mathematica | PRODUCT TRIAL
Learning Center | Help | Contact Us | Buy Mathemat
WolframAlpha
In[12]:= FactorInteger[123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3]
Wolfram|Alpha doesn't know how to interpret your input.
WolframAlpha
In[13]:= FactorInteger[55]
Input interpretation:
factor 55
Prime factorization:
5×11 (2 distinct prime factors)
Divisors:
1 | 5 | 11 | 55 (4 divisors)

Sources

- http://wri-irg.org/node/10781
- http://www.usc.edu/dept/molecular-science/RSApics.htm
- http://donpiorsuerte.wordpress.com/2010/05/21/vigenere-cipher/