Discrete Math and Abstract Algebra: Applications in Internet Security

An Awesome Presentation by Matthew Milone

What is encryption?

- Encryption is the process of encoding a message so it cannot be read by an unintended recipient.
- Encryption has been used throughout history to protect military secrets and other important information.
- If a message is encrypted well, it is extremely difficult to decode — unless you already know the proper process needed to decrypt it.

Why is it important today?

- Every day, we send out important information through the Internet — emails, bank account balances, credit card numbers, and more!
- Do you really want this guy to steal your identity?

How can we protect our data?

- Because we exchange private data with countless parties every day, it is impossible to have a predetermined encryption and decryption process unique to each party.
- In 1977, MIT students Ron Rivest, Adi Shamir, and Leonard Adleman published their work on an encryption system called RSA, after their last initials.

The Basics of RSA Encryption

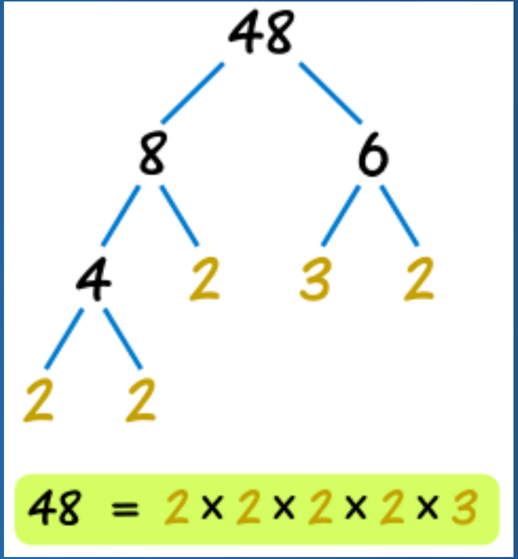
- The two parties exchanging information each have two keys: a public (shared) key for encryption and a unique private key for decryption.
- Even if a third party intercepts the encrypted message, they cannot decrypt it without access to the private keys!

How is this possible?

- Mathematics makes it possible!
- Encryption and decryption are mathematical functions.
- Encryption is a fairly simple and easy function; decryption is its inverse function and is much more difficult to perform.
- Can you think of any inverse function pairs with this same property?

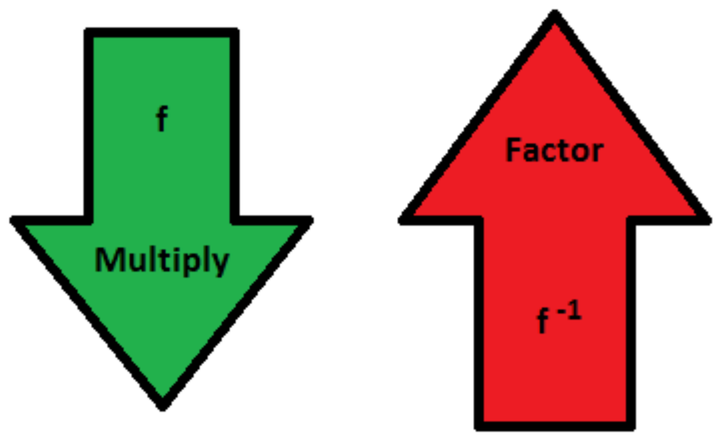
Simple Arithmetic!

- RSA encryption is based on the Fundamental Theorem of Arithmetic, which states:
  - Every positive integer (except the number 1) can be represented in exactly one way apart from rearrangement as a product of one or more primes (Wolfram Mathworld).
- What does this mean?
  - Simply stated, this means that every positive integer greater than 1 has a unique prime factorization.
- Easy so far… right?!

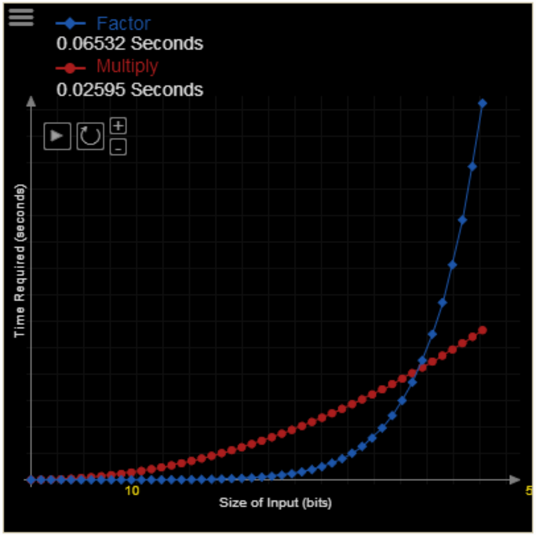


The Power of Primes

- We will now look at a type of function that is easy to perform, but has an inverse operation which is much more difficult and time-consuming.
  - It is relatively easy to multiply two prime numbers together; a computer can do this quickly, even if the numbers are very large.
  - A computer can also determine whether or not a large number is prime in a very short period of time.
  - Given a very large composite number, a computer is unable to find its prime factorization quickly; there is no known efficient algorithm.



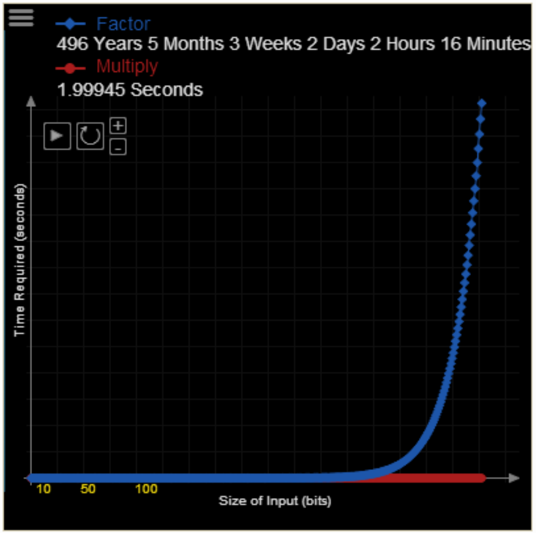
How long does it take?



45-bit key

Less than a second

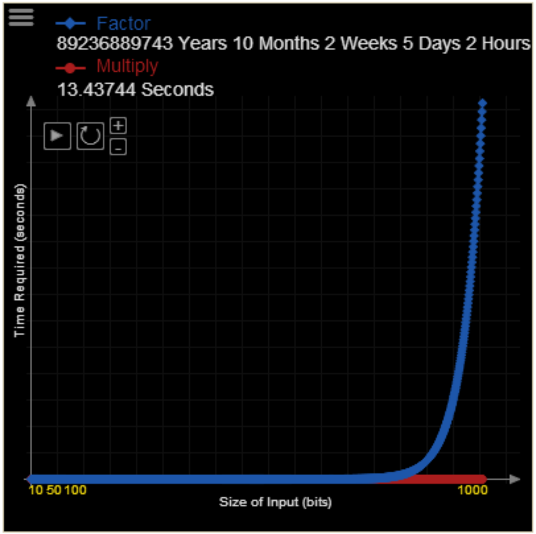
(Not a long time)



395-bit key

~500 years

(A long time)



1024-bit key

89 billion years

(~7 times age of Universe)

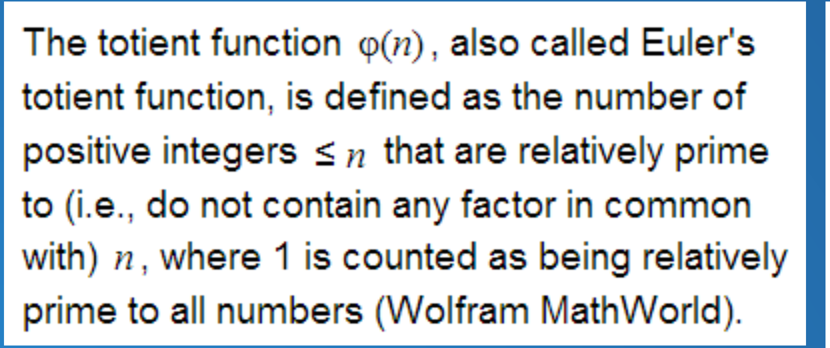
Modular Arithmetic Review

Modular arithmetic is a system of arithmetic in which numbers “wrap around” when we reach a number known as the modulus. We start by performing the operation, then dividing the answer by the modulus and taking the remainder. It might be helpful to visualize a clock:

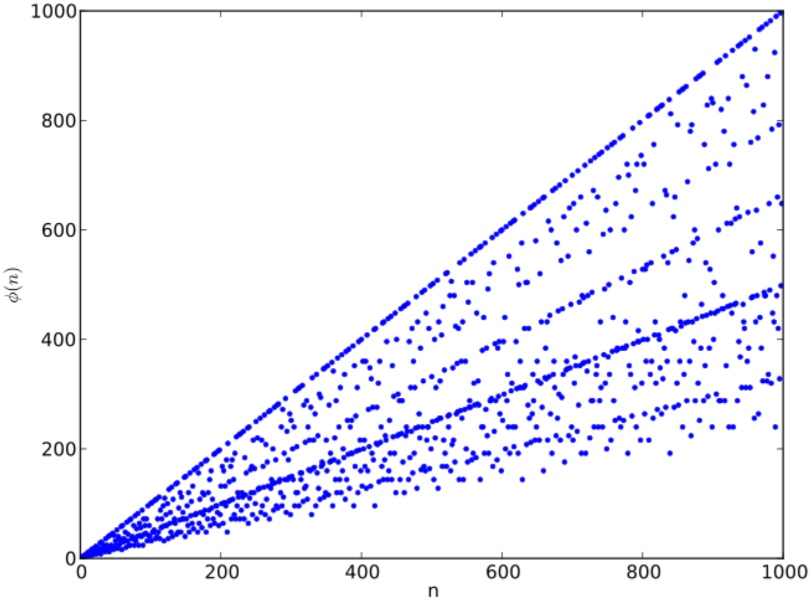
- If it is 8 o’clock and we want to add 7 hours, we get:
- $8 + 7 \equiv 15 \pmod{12} \equiv 3$

RSA Encryption, along with many other processes in computing, relies heavily on modular arithmetic.

Euler's Totient Function



The totient function $\varphi(n)$, also called Euler's totient function, is defined as the number of positive integers $\leq n$ that are relatively prime to (i.e., do not contain any factor in common with) n, where 1 is counted as being relatively prime to all numbers (Wolfram MathWorld).

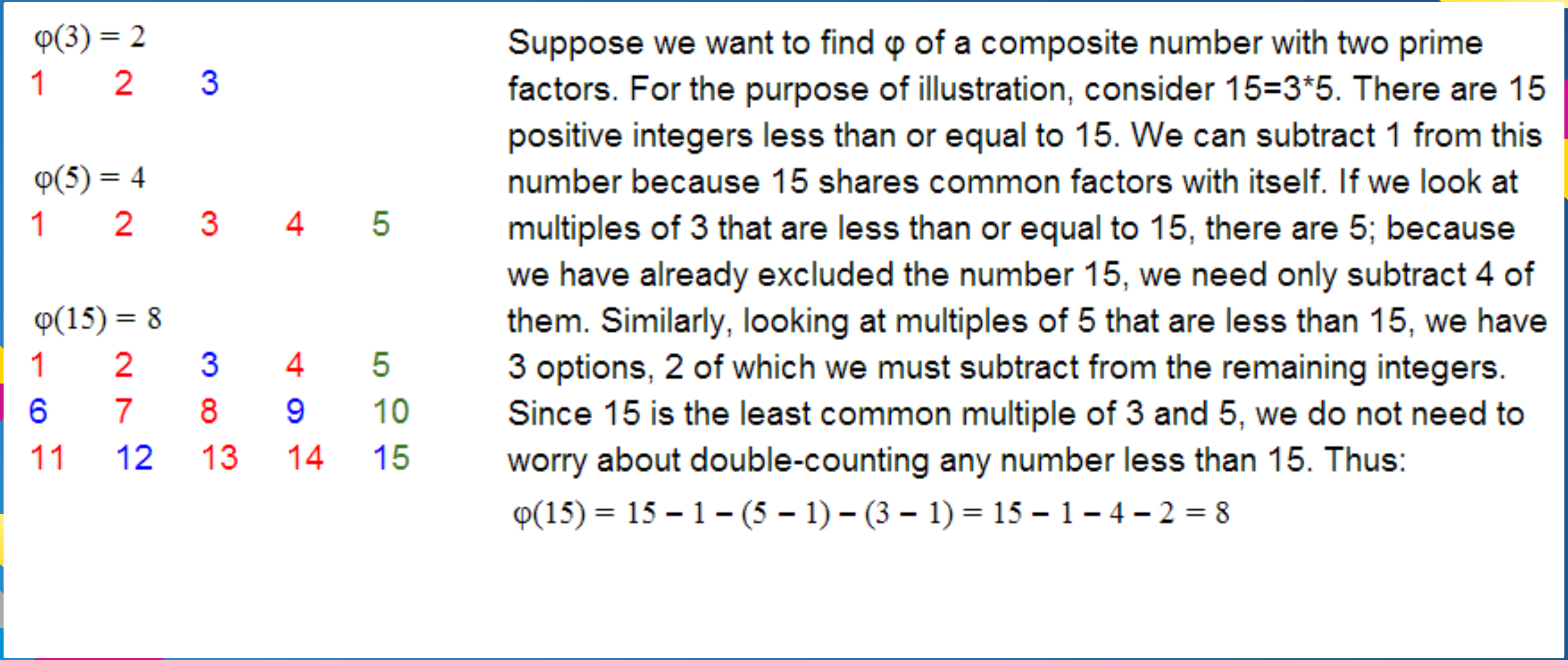


The graph to the right shows the first thousand values for φ(n).

Useful Properties of φ(n)

- φ(n) has a couple of properties that are useful in the RSA encryption and decryption processes:
    - A prime number has no factors except for one and itself. Therefore, if n is prime, φ(n)=n-1.
    - If two numbers a and b are relatively prime, then φ(n) is multiplicative. This means that φ(a*b)=φ(a)*φ(b).

Calculating φ(n)



$\varphi(3) = 2$

1	2	3

$\varphi(5) = 4$

1	2	3	4	5

$\varphi(15) = 8$

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15

Suppose we want to find φ of a composite number with two prime factors. For the purpose of illustration, consider 15=3*5. There are 15 positive integers less than or equal to 15. We can subtract 1 from this number because 15 shares common factors with itself. If we look at multiples of 3 that are less than or equal to 15, there are 5; because we have already excluded the number 15, we need only subtract 4 of them. Similarly, looking at multiples of 5 that are less than 15, we have 3 options, 2 of which we must subtract from the remaining integers. Since 15 is the least common multiple of 3 and 5, we do not need to worry about double-counting any number less than 15. Thus:

$$\varphi(15) = 15 - 1 - (5 - 1) - (3 - 1) = 15 - 1 - 4 - 2 = 8$$

Multiplicative Property of φ(n)

We can generalize this formula for any number *ab* that is the multiple of two different prime numbers, *a* and *b*:

$\varphi(15) = 15 - 1 - (5 - 1) - (3 - 1) = 15 - 1 - 4 - 2 = 8$

$\varphi(a*b) = ab - 1 - (a - 1) - (b - 1) = ab - a - b + 1$

Since *a* and *b* are prime, we can also say:

$\varphi(a) = a - 1$

$\varphi(b) = b - 1$

If φ is multiplicative, then $\varphi(a*b)=\varphi(a)*\varphi(b)$ must hold true.

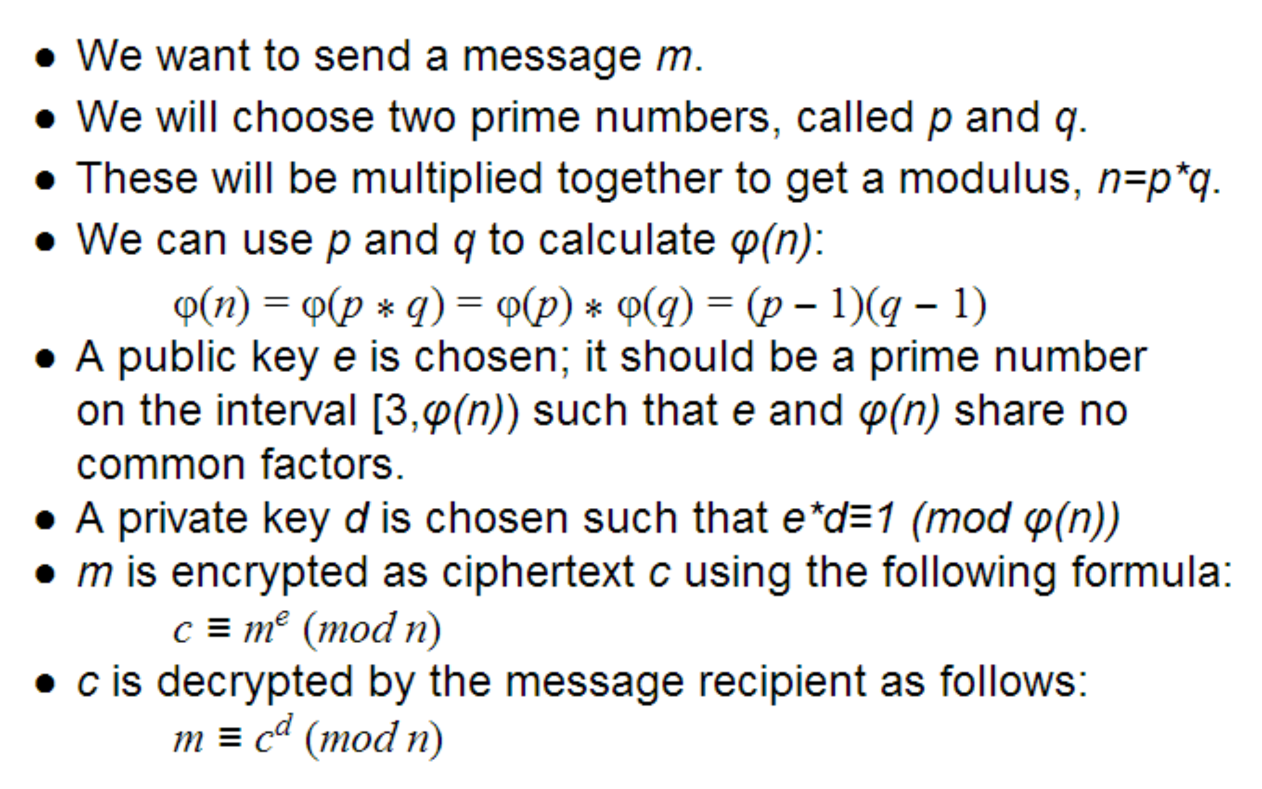
$\varphi(a*b)=\varphi(a)*\varphi(b)$

$ab - a - b +1 = (a - 1)(b - 1)$

$ab - a - b +1 = ab - a - b +1$

This is true; φ is multiplicative when *a* and *b* are prime, a≠b.

Variables and Formulas



- We want to send a message *m*.
- We will choose two prime numbers, called *p* and *q*.
- These will be multiplied together to get a modulus, *n=p*q*.
- We can use *p* and *q* to calculate *φ(n)*:

$$\varphi(n) = \varphi(p * q) = \varphi(p) * \varphi(q) = (p - 1)(q - 1)$$

- A public key *e* is chosen; it should be a prime number on the interval [3,*φ(n)*) such that *e* and *φ(n)* share no common factors.
- A private key *d* is chosen such that *e*d≡1 (mod φ(n))*
- *m* is encrypted as ciphertext *c* using the following formula:

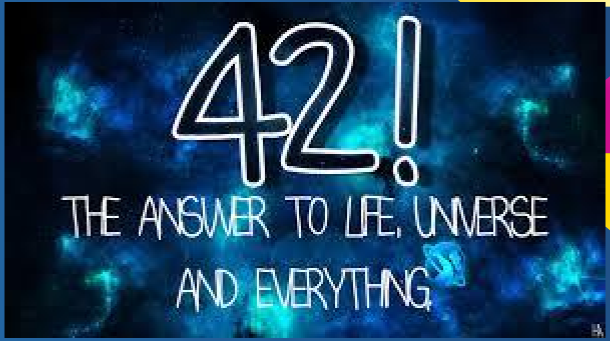
$$c \equiv m^e \ (mod\ n)$$

- *c* is decrypted by the message recipient as follows:

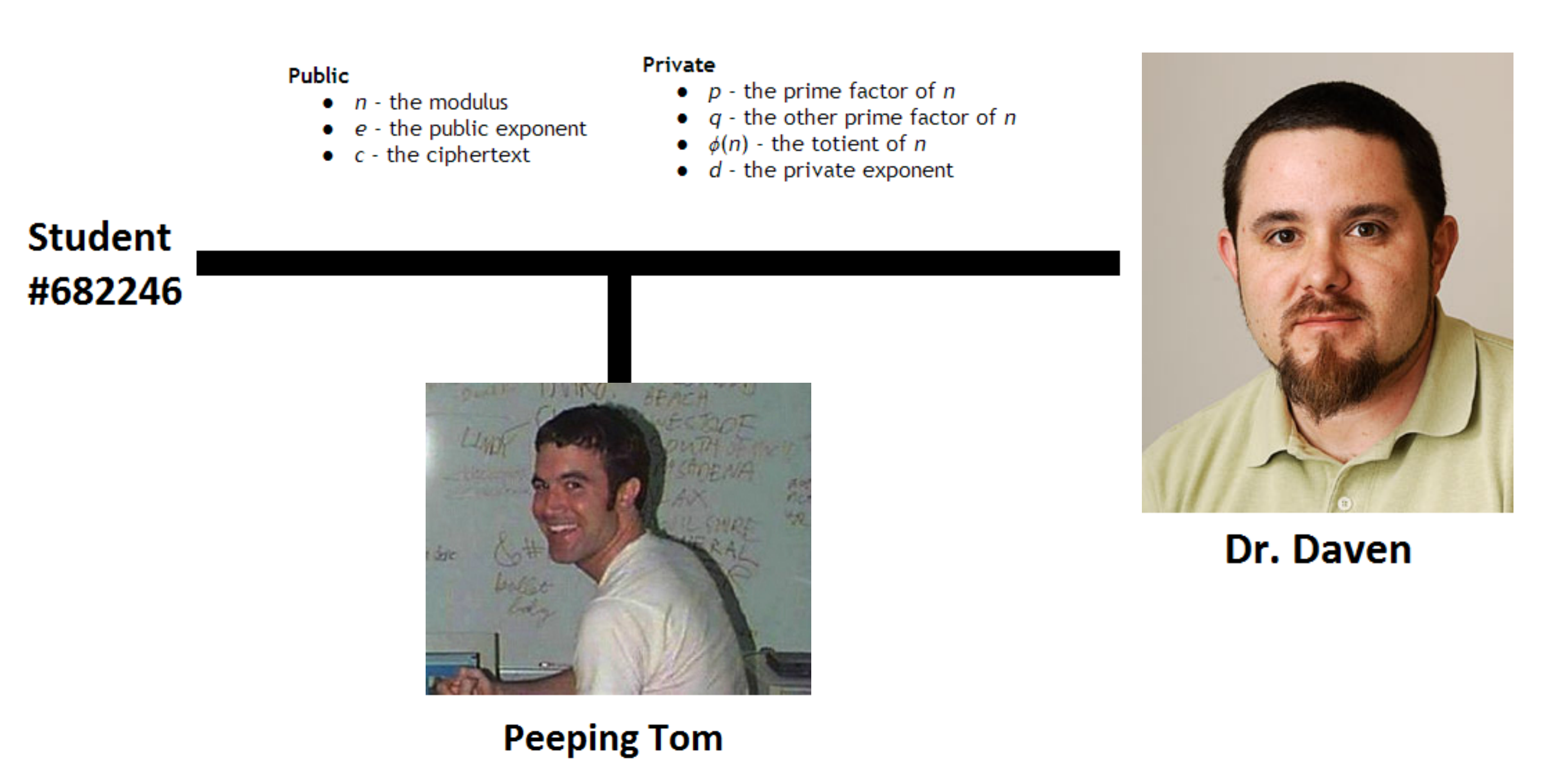
$$m \equiv c^d \ (mod\ n)$$

A Working Example

Dr. Daven assigns a Homework Alpha problem in which Student #682246 is asked to calculate the answer to life. Student #682246 quickly determines that the answer to life is 42, and wants to email this information to Dr. Daven. Using RSA encryption, Student #682246 is able to do so without prying eyes stealing his answer. Let's take a closer look:



A View of the Network



Public

- n - the modulus
- e - the public exponent
- c - the ciphertext

Private

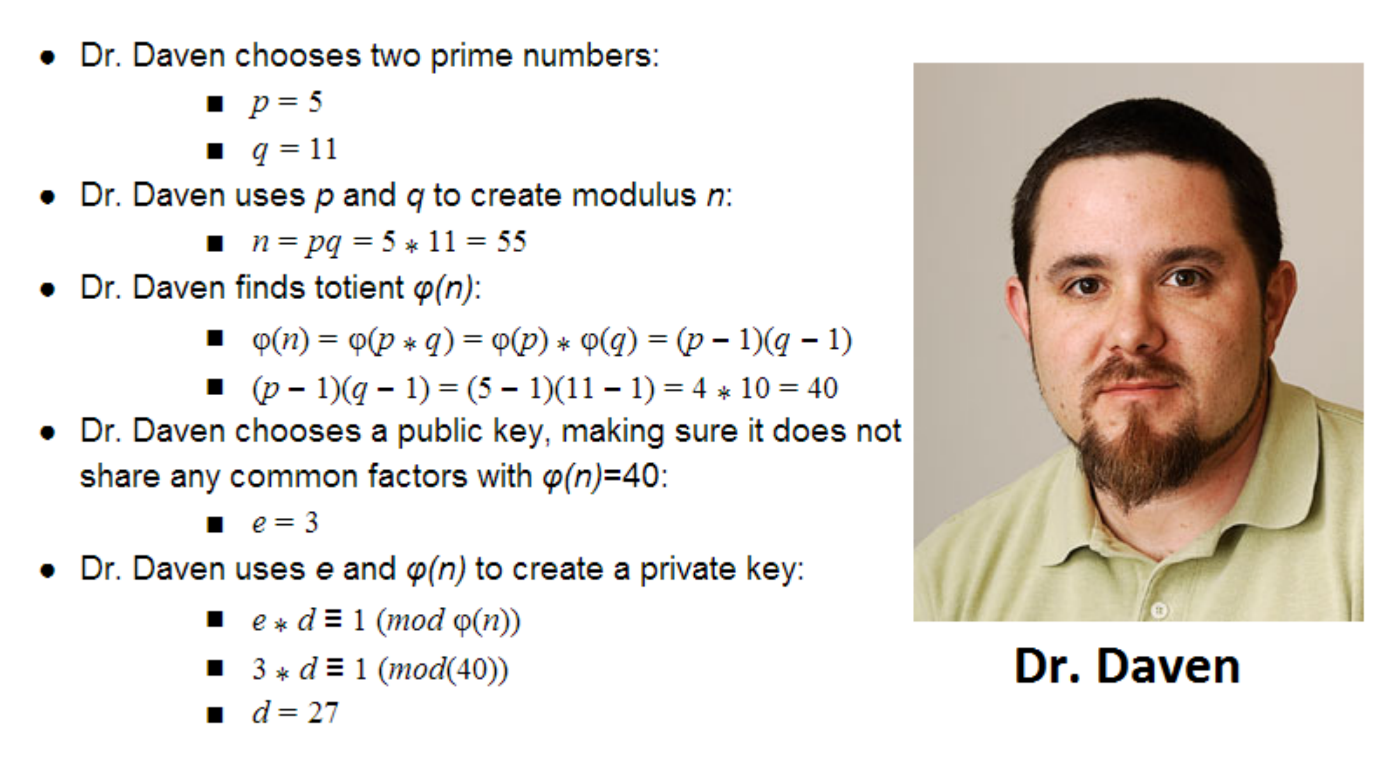
- p - the prime factor of n
- q - the other prime factor of n
- $\phi(n)$ - the totient of n
- d - the private exponent

Student #682246

Peeping Tom

Dr. Daven

Encryption



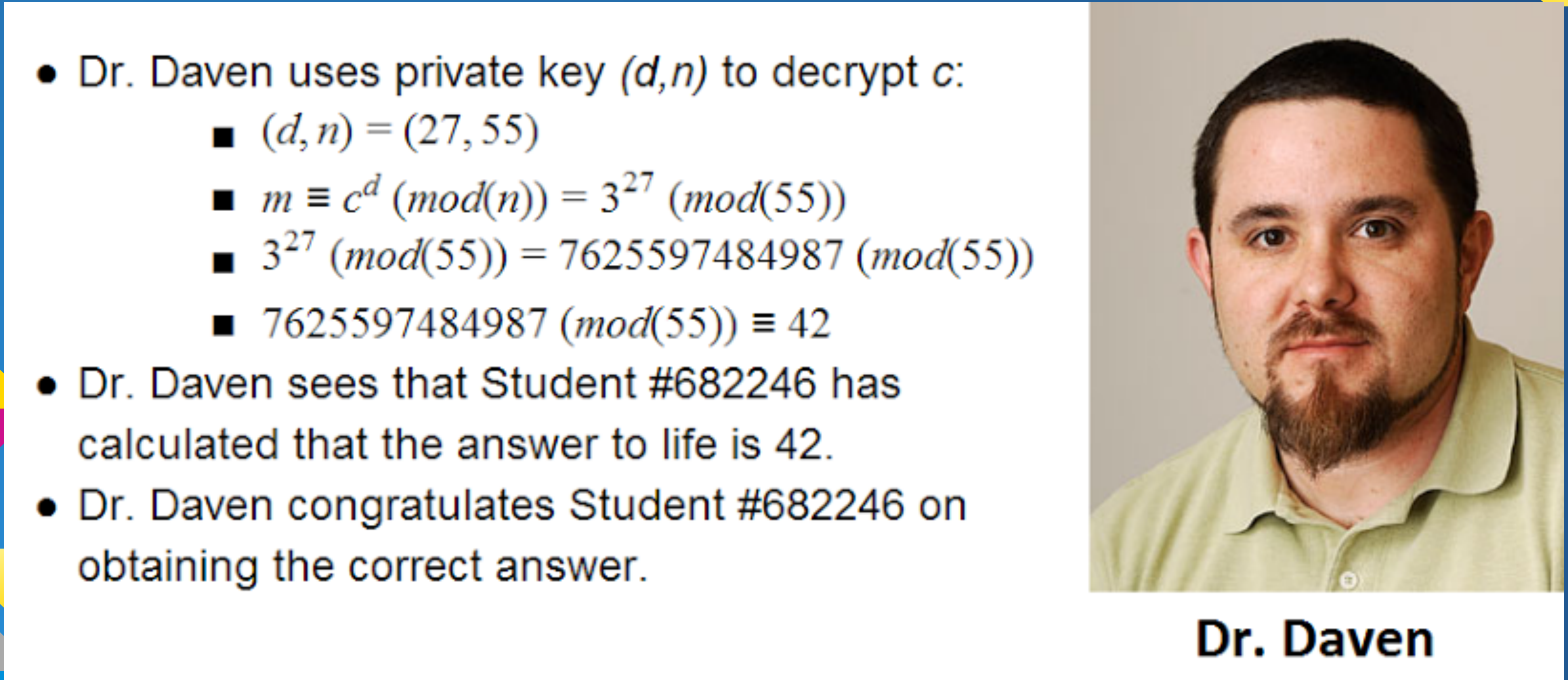
- Dr. Daven chooses two prime numbers:
  - $p = 5$
  - $q = 11$
- Dr. Daven uses *p* and *q* to create modulus *n*:
  - $n = pq = 5 * 11 = 55$
- Dr. Daven finds totient *φ(n)*:
  - $\varphi(n) = \varphi(p * q) = \varphi(p) * \varphi(q) = (p - 1)(q - 1)$
  - $(p - 1)(q - 1) = (5 - 1)(11 - 1) = 4 * 10 = 40$
- Dr. Daven chooses a public key, making sure it does not share any common factors with *φ(n)*=40:
  - $e = 3$
- Dr. Daven uses *e* and *φ(n)* to create a private key:
  - $e * d \equiv 1\ (mod\ \varphi(n))$
  - $3 * d \equiv 1\ (mod(40))$
  - $d = 27$

Dr. Daven

Encryption, Continued

- Dr. Daven sends public key *e* and modulus *n* to Student #682246 as public key *(e,n)*:
    - $(e, n) = (3, 55)$
- Student #682246 takes message *m*=42 and encrypts it as ciphertext *c*:
    - $c \equiv m^e\ (mod(55)) = 42^3\ (mod(55))$
    - $42^3\ (mod(55)) = 74088\ (mod(55)) \equiv 3$
- Student #682246 sends ciphertext *c*=3 back to Dr. Daven.

Decryption



- Dr. Daven uses private key *(d,n)* to decrypt *c*:
  - $(d, n) = (27, 55)$
  - $m \equiv c^{d}\ (mod(n)) = 3^{27}\ (mod(55))$
  - $3^{27}\ (mod(55)) = 7625597484987\ (mod(55))$
  - $7625597484987\ (mod(55)) \equiv 42$
- Dr. Daven sees that Student #682246 has calculated that the answer to life is 42.
- Dr. Daven congratulates Student #682246 on obtaining the correct answer.

Dr. Daven

Breaking the Encryption...

- Peeping Tom has a problem:
  - He does not respect people’s privacy.
  - He also has a mathematical problem.
- Peeping Tom knows the following:
  - $c = 3$
  - $n = 55$
  - $e = 3$
  - $m \equiv c^d \ (mod(n)) = 3^d \ (mod(55))$

Peeping Tom

...or not!

- To calculate d, Peeping Tom needs to know $\varphi(55)$ so he can use it in the equation $3*d \equiv 1 \bmod(\varphi(55))$.
- The best method for calculating $\varphi(55)$ that Peeping Tom knows is by finding its prime factors p and q, then using the equation $\varphi(n)=\varphi(p*q)=\varphi(p)*\varphi(q)=(p-1)(q-1)$ to find the totient.
- Finding prime factorizations takes too long.
- Dr. Daven and Student #682246 have thwarted Peeping Tom once and for all!

Peeping Tom

Is it really secure?

- Of course, anyone in this room could find the prime factors of 55 quickly…
- But what if we use larger numbers?
- What is the prime factorization of 11,843,119?
- It’s 2341 x 5059.
- How did I figure that out?
- I cheated. I found the two prime numbers first, and then multiplied them to get 11,843,119.
- Encryption keys are generally much larger than 11,843,119… so your data is safe!

Credits

http://doctrina.org/How-RSA-Works-With-Examples.html

http://doctrina.org/Why-RSA-Works-Three-Fundamental-Questions-Answered.html#wruiwrtt

http://en.wikipedia.org/wiki/File:EulerPhi.svg

https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/p/time-complexity-exploration

http://mathworld.wolfram.com/FundamentalTheoremofArithmetic.html

http://mathworld.wolfram.com/TotientFunction.html

Special Thanks

- Dr. Daven, for helping me get started when I did not know where to go with this project. Also for making numerous cameo appearances throughout this presentation.
- Dr. Fothergill, for giving me the ideas I needed to take this topic further and make it more interesting.
- Robbie, whose bowl of candy was my primary source of sustenance while I worked on putting this together.
- Taylor and Maggie, who provided me with both emotional support and comic relief when I thought this project was going to cause me to have a complete nervous breakdown.
- The best image editing software ever created, MS Paint.

The End

So remember, be sure to use powerful encryption methods for important data such as your Death Star plans… It never ends well when the Rebels who steal them can also read them.

(I used this picture in the last slide because I wanted to go out with a bang.)