Shift and Vigenere

Tuesday, July 11, 2023 2:28 PM

Objectives:

1. Intro
2. Syllabus
3. Crypto Basics

Alice

162 = m

m + 111 = c = 273 ⟶

k

Eve

m + k = c

c - k

CCT

Ciphertext Only

kPT

CPT

m + k = c

c = 273

m = ?

k = ?

Alice

k = 10

m = "h"

↓

7

C = m + k = 17

Eve

k = 10

R ⟶ R

22 + 10 (mod 26) = 6 ⟶ 6 - 10 =

CAR k = 13

Vigenere Cipher

Alice Eve

k = (1, 10, 3, 16)

h	e	l	l	o	w	o	r	l	d	e	e	e	e	e	e
7	4	11	11	14	22	14	17	11	3	4	4	4	4	4	4
1	10	3	16	1	10	3	16	1	10	3	16	1	10	3	16
8	14	14	1	15	6	17	7	12	13	2	20	5	14	7	20
I	O	O	B	P	G	R	H	M	N	H	U	F	O	H	U

Vigenere and Affine

Monday, August 21, 2023 2:47 PM

Vigenere Cipher

$k = (1, 10, 3, 16)$

h e l l o w o r l d e e e e e e e e

7 4 11 11 14 22 14 17 11 3 4 4 4 4 4 4 4

1 10 3 16 1 10 3 16 1 10 3 16 1 10 3 16 1

8 14 14 1 15 6 17 7 12 13 2 20 5 14 7 20 5

I O O B P G R H M N H U F O H U F

Shift

0

I O O B P G R H M N H U F O H U 1 — 1

I O O B P G R H M N H U F O H 2

I O O B P G R H M N H U F O 1 — 3

I O O B P G R H M N H U F 3 — 4

I O O B P G R H M N H U 5

I O O B P G R H M N H 6

I O O B P G R H M N 7

$k = 1, 10, 3, 16$

I P M F F

O G N O

O R H H

B H U U

Affine Cipher

$k = (9, 2)$

$a = 9$

13 = 2

h

↓

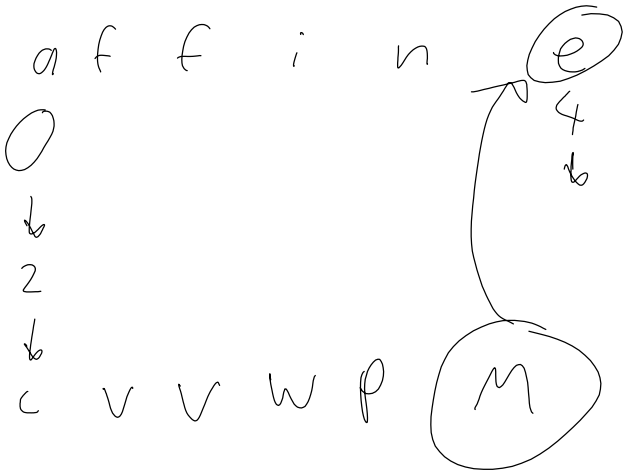
7

N

↑

$7 \cdot 9 + 2 \pmod{26} \equiv 13$

$0 \cdot 9 + 2 \pmod{26} \equiv$



a → C e → M

0 → 2 4 → 12

$0 \cdot \alpha + \beta = 2$ $\beta = 2$

$4 \cdot \alpha + \beta = 12$

$4 \cdot \alpha = 10 \pmod{26}$

$4 \cdot \alpha = 36$

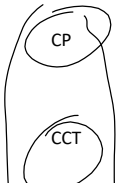
$\alpha = 9$

INPUT

ALTER

$\alpha = 13 \quad \beta = 4$

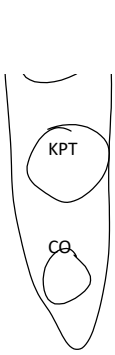
ERRER



LTBNSFXBIQ

You can as me to encrypt 2 plain text letters

See Solutions



QWCYFSMCRX

You can ask me to decrypt 2 cipher text letters

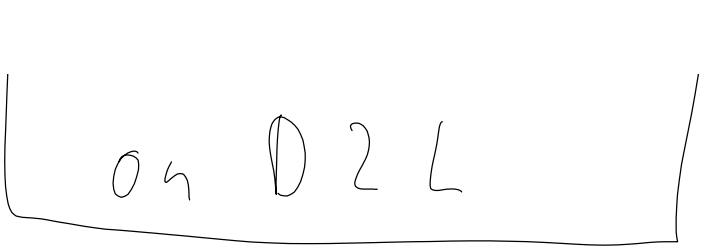
XGFKCZ

b->M c->X

LRGVI

Most common letter in the text (e) ->V

Second most common letter in the test (t) ->S



Substitution, Enigma and XOR

Wednesday, August 23, 2023 10:55 AM

Substitution ciphers

How many possible keys exist for a shift cipher?

25

Vigenere with a key length of 4?

26^4

Affine cipher?

$(13-1)(2-1) = 12$ for α

12 · 26

Example

Plain text abcdefghijklmnopqrstuvwxyz

Cipher key QPQRABGHIJKLMNSTUVWXYZCDEF

Encyrpt "cat"

26!

"QOX"

Decrypt "RSG"

"dog"

How would you break it?

Enigma

Demo: Enigma Machine Emulator - 101 Computing

How many "keys"?

Rotors 5 · 4 · 3

Roter setting 26^3

Plugboard setting 26!/(6!10!2^10)

Total: 158,962,555,217,826,360,000

158 quintillion 962 quadrillion 555 trillion 217 billion 826 million 360 thousand

What are the strengths of the enigma?

QUZ BFU

Weaknesses:

Plain text was never encrypted to itself.

Cycles were looked for and catalogued.

3 letter code sent twice.

SIGABA (American – 5(+5) rotors) and Typex (British – 7 rotors)

Neither was broken.

XOR

Binary Numbers and ASCII

table 0x30 -> 0, 0x41 -> A, 0x61 -> a

XOR

```
cg -> 99 103-> 0110 0011 0110 0111
Key            0100
Cipher text
Key
Result
```

How would you break it? (What other cipher is this similar to?)

One time pad

```
cg -> 99 103-> 0110 0011 0110 0111
Key            0100
```

Key length = message length

Security guarantee

If I receive a 0, what is the probability that a 1 was sent?

What about a 0?

What if I receive a 1?

Pseudo- random bit generation – this is hard

Block Ciphers

Diffusion –

A plaintext = big A in ciphertext

Confusion –

DES – Block size 64 bits

Key size 56 bits

AES – Block size 128 bits

Key sizes 128, 192, 256 bits

What is the CIA triad?

C

I

A

What 2 things often get added?

So far what have these ciphers so far been doing?

Cryptography can help with all these tasks:

Confidentiality –

Integrity –

Availability –

Authenticity –

Non-repudiation –

Primality and Divisibility

Monday, August 28, 2023 11:48 AM

Divisibility: a divides b (a|b) means there exists an integer k such that b = ak

If a|b and b|c then a|c

Why? $b = ak$ $c = bi$ $c = a(ki)$

Prime Number: p > 1 s.t. only divisible by 1 and p

What are some prime numbers? 2, 3, 5

Not prime -> composite

Relatively Prime

2 Numbers, a and b where GCD(a,b) = 1

Exercise

Two primes that are relatively prime:

Prime and composite that are relatively prime: 2, 5

Prime and composite that are not relatively prime: 3, 6

2 composites that are relatively prime: 3, 6

2 composites that are not relatively prime: 4, 6

Two primes that are not relatively prime: 2, 4

Primes building blocks of numbers

Fundamental Theorem of Arithmetic: Every positive integer is the unique product of primes (up to a reordering of the factors)

$n = p^a{}_1 p^b{}_2 p^c{}_3 \ldots p^g{}_n$

Exercise: Prime factorization of class years – Online tools exist for this. Express factors in increasing order.

$3^4 \cdot 5^2$

Euclidean Algorithm and the Extended Euclidean Algorithm

Tuesday, August 29, 2023 2:30 PM

The GCD is the largest number that divides both.

GCD(35,7) = 7

GCD(12,17) = 1

GCD(5,11) = 1

If p_1 and p_2 are prime numbers, what is GCD(p_1,p_2)? 1

If m_1 and m_2 are coprime (relatively prime), what is GCD(m_1,m_2)? 1

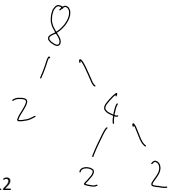
How do we go about computing the GCD for two numbers?

Compare Factorizations (brute force)

Factor the numbers, pick out all the factors that match, multiply them together to get GCD

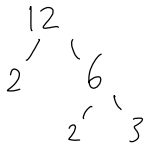
Example #1

Factor 8



$2^3 = 2^2 \cdot 2$

Factor 12



$2^2 \cdot 3$

What factors match?

2^2

What is the GCD?

4

Example #2

A = $2^2 \times 3 \times 7^3 = 4116$

~~B = $2 \times 5 \times 7^2 \times 13 = 6370$~~

What is GCD(4116,6370)?

$2 \cdot 7^2 = 98$

Euclidean Algorithm – Recursive algorithm for solving GCD

GCD(a,b) = ? Step 0 swap a and b if needed to put the larger one first.

Step 1: divide a by b to get a = b(q) + r

If r = 0 THEN b is the GCD of a and b.

Repeat Step 1 with a <- b and b <- r and continue this way until r = 0

Do example with GCD(12,105)

$105 = 12 \cdot 8 + 9$

$12 = 9 \cdot 1 + 3$

$9 = 3 \cdot 3 + 0$

This leads to the Extended Euclidean Algorithm – Solving Ax + By = D, where D = GCD (A,B)

This form is useful if D = 1 because:

B * y ≡ 1 (mod x)

B * y ≡ 1 (mod A)

A * x ≡ 1 (mod y)

A * x ≡ 1 (mod B)

Why are these equasions useful?

Examples

GCD (105,12)

$105 = 12 \cdot 8 + 9$

$12 = 9 \cdot 1 + 3$

$9 = 3 \cdot 3 + 0$

$105 + 12 \cdot -8 = 9$

$12 + 9 \cdot -1 = 3$

$9 - 3 \cdot 3 = 0$

$(0)\,105 + (1)\,12$

$Ax + By = D$

$(1)105 + (-8)12 = 9$

$(0)\,105 + (1)\,12 + (-1)\left((1)105 + (-8)12\right)$

$(-1)\,105 + (9)\,12 = 3$

A x + B y

$(0)128 + 13(1) = 13$

GCD (128,13)

x y

$128 = 13 \cdot 9 + 11$

$13 = 11 \cdot 1 + 2$

$11 = 2 \cdot 5 + 1$

$2 = 1 \cdot 2 + 0$

$128 + 13(-9) = 11$

$13 + 11(-1) = 2$

$11 + 2(-5) = 1$

$(1)\,128 + (-9)\,13 = 11$

$13 + (-1)\left((1)128 + (-9)13\right) = 2$

$(-1)128 + (10)13 = 2$

$A \times + B \times y = D$

$(1)128 + (-9)13 + (-5)\left((-1)128 + (10)13\right) = 1$

$(6)128 + (-59)13 = 1$

$13^{-1} = -59 \equiv 69 \pmod{128}$

Practice problems

GCD(12,17)

$17 = 12 \cdot 1 + 5 \rightarrow 17 + 12(-1) = 5$

$12 = 5 \cdot 2 + 2 \rightarrow 12 + 5(-2) = 2$

$5 = 2 \cdot 2 + 1 \rightarrow 5 + 2(-2) = 1$

$2 = 1 \cdot 2 + 0$

$12 + \left((1)17 + (-1)12\right)(-2) = 2$

$12 + (-2)17 + (2)12 = 2$

$(-2)17 + (3)12 = 2$

Find $12^{-1} \pmod{17}$

$(1)17 + (-1)12 = 5$

$(-2)17 + (3)12 = 2$

$(5)17 + (-7)12 = 1$

$12^{-1} \equiv -7 \equiv 10 \pmod{17}$

$(1)17 + (-1)12 + (-2)\left((-2)17 + (3)12\right) = 1$

$(1)17 + (-1)12 + (9)17 + (-6)12 = 1$

$(5)17 + (-7)12 = 1$

GCD(5,11)

$11 = 5 \cdot 2 + 1 \rightarrow 11 + 5 \cdot (-2) = 1$

$5 = 1 \cdot 5 + 0$

Find $5^{-1} \pmod{11}$

$A \times + B y = 2$

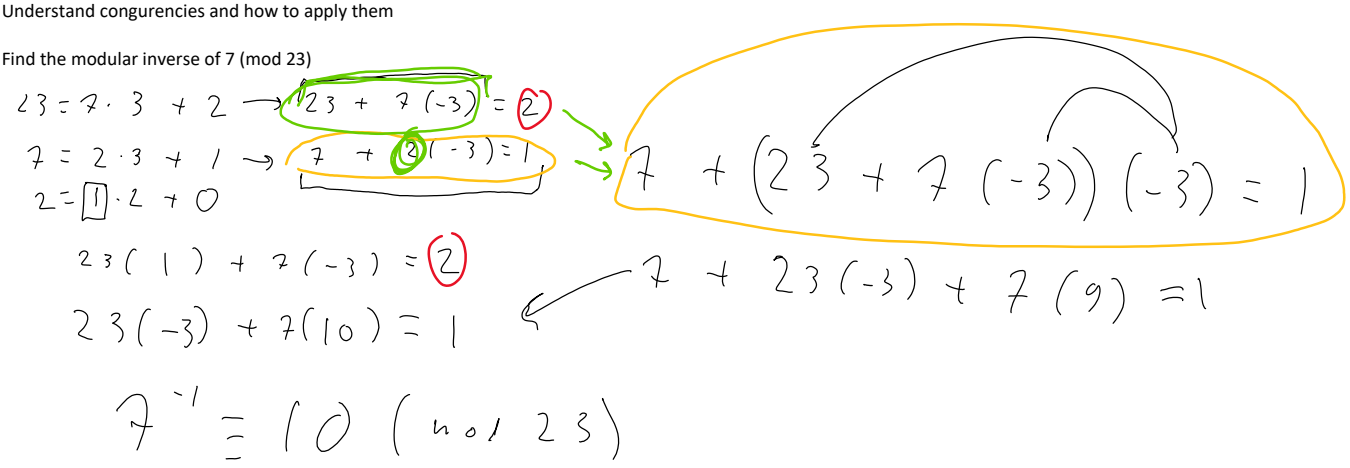
$(1)\ 11 \times + (-2)5 = 1 \qquad -2 \equiv 9 \pmod{11}$

Congruences

Wednesday, August 30, 2023 9:25 AM

Goals for today:
Practice Extended Euclidian Algorithm
Understand congurencies and how to apply them

Find the modular inverse of 7 (mod 23)



For all integers a and b, we can always find integers x and y such that ax + by = d where d = GCD(a,b).

If a and b are given,

Use the Euclidean algorithm to find: d

Use the Extended Euclidean algorithm to find: x, y

If d = 1 we can compute: find mod inv

Let's look at some other properties of modulus math

8 + 14 ≡ 1 mod 7

8 mod 7 + 14 mod 7 ≡ 1 mod 7

8 x 14 ≡ 0 mod 7

(8 mod 7) * (14 mod 7) ≡ 0 mod 7 = 1 · 0 = 0

Tells us 2 things:

(1) Big numbers can be reduced before calculations are made

Why is this important?

(2) Equivalence Classes

Example (mod 7)

	0	1	2	3	4	5	6
Row 1	7	8	9	10	11	12	13
2	14	15	16	17	18	19	20
3	-7	-6	-5	-4	-3	-2	-1
4	777	778	779	280	281	282	283

[1] + [2] =

Row 1: 9 + 9 ≡ 3 (mod 7)

Row 2: 15 + 16 ≡ 3 (mod 7)

Row 3: -6 + -5 ≡ 3 (mod 7)

Row 4: 3

[2] x [3] =

Row 1:

Row 2: 6

Row 3: 6

Row 4: 6

Assume GCD(a,n) = 1

How would you solve ax ≡ b mod n?

Example $9x \equiv 5 \bmod 17$

Use Excel Spreadsheet to find $1111x \equiv 27 \bmod 4568$

If GCD(a,n) ≠1 -> More than one solution (or none)

1. Find GCD(a,n) = d Check to see if d | b.
   1. IF No THEN No solution.
   2. IF Yes THEN divide a,b,n by d and ~~solve for~~ x0.
2. Remaining solutions are x0 + kn/d for k = 0,1,2,... d-1

Example

$24x \equiv 12 \bmod 51$

$51 = 24 \cdot 2 + 3$

$24 = (3) \cdot 8 + 0$

$\frac{24}{3} x \equiv \frac{12}{3} \pmod{\frac{51}{3}} \rightarrow 3$ solution

$8x \equiv 4 \pmod{17}$

$17 = 8 \cdot 2 + 1 \rightarrow 17 + 8(-2) = 1$

$8 = (1) \cdot 8 + 0$

$17(1) + 8(-2) = 1$

$8^{-1} \equiv -2 \equiv 15 \pmod{17}$

$15 \cdot 8x \equiv 4 \cdot 15 \pmod{17}$

$x \equiv 4 \cdot 15 \equiv 9 \pmod{17}$

$x_0 = 9 \quad = 9$

$x_1 = 9 + 17 \quad = 26$

$x_2 = 9 + 17(2) \quad = 43$

$24(9) \equiv 12 \pmod{51}$

$24(26) \equiv 12 \pmod{51}$

$24(43) \equiv 12 \pmod{51}$

Check by plugging back into original congruence:

Practice Problems:

$8x \equiv 92 \pmod{20}$

$8x \equiv 12 \pmod{20}$

$8 = 4 \cdot 2 + 0$

$\frac{8}{4} x \equiv \frac{12}{4} \pmod{\frac{20}{4}}$

$2x \equiv 3 \pmod 5$

$5 = 2 \cdot 2 + 1 \rightarrow 5 + 2 \cdot (-2) = 1$

$(1)5 + (-2)2 = 1$

$2^{-1} \equiv (-2) \equiv 3 \pmod 5$

$2x \equiv 3 \pmod 5$

$2x \equiv 3 \cdot 3 \pmod 5$

$x \equiv 9 \equiv 4 \pmod 5$

$x_0 = 4 + 5(0)$

$x_1 = 4 + 5(1)$

$x_2 = 4 + 5(2)$

$x_3 = 4 + 5(3)$

9x ≡5 (mod 21)

$21 = 9 \cdot 2 + 3$

$9 = 3 \cdot 3 + 0$

3|5 ? No!

55x ≡ 50 (mod 40)

GCD = 5

$15x \equiv 10 \pmod{40}$ → divide by 5

$3x \equiv 2 \pmod 8$

$8 = 3 \cdot 2 + 2 \rightarrow 8 + 3(-2) = 2$

$3 = 2 \cdot 1 + 1 \rightarrow 3 + 2(-1) = 1$

$2 = 1 \cdot 2 + 0$

$8(1) + 3(-2) = 2$

$3 + (8 + 3(-2))(-1) = 1$

$3 + (-1)8 + 3(2) = 1$

$(-1)8 + 3(3) = 1$

$3^{-1} \equiv 3$

$3x = 2 \pmod 8$

$x \equiv 2 \cdot 3 \equiv 6 \pmod 8$

$x_0 = 6$

$x_1 = 6 + 8$

$x_2 = 6 + 8(2)$

$x_3 = 6 + 8(3)$

$x_4 = 6 + 8(4)$

CRT, Gauss' Algorithm

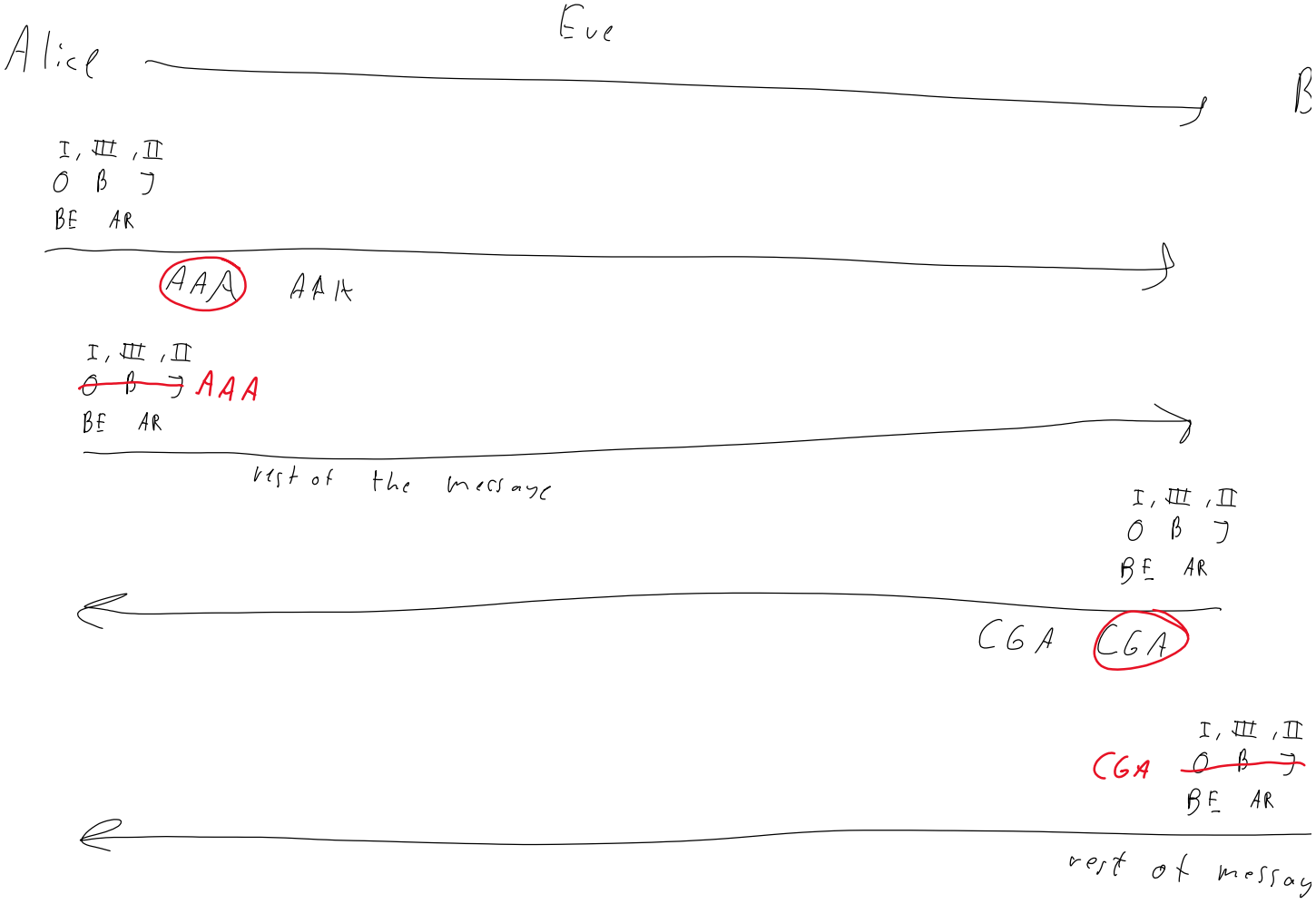
Tuesday, September 05, 2023 4:13 PM

Goals

- Homework Review
- Chinease Remainder Theoreom
- Gauss Algorithm

1. How many keys for substitution cipher?
2. Enigma review
   - Enigma "key":
     i. Rotors
     ii. Rotor setting (initial condition):
     iii. Plugboard:

I, III, II
O B J
BE AR



Chinese Remainder Theorem

Given x ≡ a mod m, & x ≡ b mod n

CRT states that there is a unique solution, x, up to mn given that GCD(m,n) = 1.

Example

Let x ≡ 3 mod 5, & x ≡ 1 mod 2

GCD(5,2) = 1

Therefore 1 unique solution(s) up to mn 2 · 5 = 10

Since x ≡ 3 mod 5:

$x \in (3, 8)$

Since x ≡ 1 mod 2:

$x \in (1, 3, 5, 7, 9)$

$x \equiv 3 \pmod{10}$

$x = 3 + k \cdot 10$

Shortcut:

Let x ≡ 3 mod 5, & x ≡ 1 mod 2, & x ≡ 2 mod 3

GCD(5,3) = 1

GCD(5,2) = 1

GCD(3,2) = 1

Therefore 1 unique solution(s) up to 30

$3 \cdot 2 \cdot 5$

$2 \not\equiv 1 \pmod 2$ $\quad 3 \equiv 1 \pmod 2$

$2 + 3 = 5 \equiv 1 \pmod 2$ $\quad 3 + 2 \cdot 5 = 13 \not\equiv 2 \pmod 3$

$5 \not\equiv 3 \pmod 5$ $\quad 3 + 2 \cdot 5(2) = \boxed{23} \equiv 2 \pmod 3$

$5 + 2 \cdot 3 = 11 \not\equiv 3 \pmod 5$

$5 + 2 \cdot 3(2) = 17 \not\equiv 3 \pmod 5$

$5 + 2 \cdot 3(3) = \boxed{23} \equiv 3 \pmod 5$

Try: x ≡ 3 mod 5, x ≡ 14 mod 17 $\quad 5 \cdot 17 = 85 \quad x < 85$

$3 \not\equiv 14 \pmod{17}$

$8 \not\equiv 14 \pmod{17}$

$13 \not\equiv 14 \pmod{17}$

$18 \not\equiv 14 \pmod{17}$

$23 \not\equiv 14 \pmod{17}$

$28 \not\equiv 14 \pmod{17}$

33

38

43

$\boxed{48} \equiv 14 \pmod{17}$

Gauss' Algorithm

Example: x ≡ 3 mod 5, x ≡ 14 mod 17

GCD(5,17) = 1

Therefore 1 unique solution(s) up to $5 \cdot 17 = 85$

$17^{-1} \bmod 5 =$

$17 = 5 \cdot 3 + 2 \rightarrow 17(1) + 5(-3) = 2$

$5 = 2 \cdot 2 + 1 \rightarrow 5 + 2 \cdot (-2) = 1$

$2 = \boxed{1} \cdot 2 + 0$

$17(1) + 5(-3) = 2$

$\boxed{17(-2) + 5(7) = 1}$

$5 + (17(1) + 5(-3)) \cdot 2 = 1$

$5 + 17(-2) + 5(6) = 1$

$-2 \equiv \boxed{3} \pmod 5$

$5^{-1} \bmod 17 = 7$

$x \equiv 3 \pmod 5 \quad x \equiv 14 \bmod 17 \quad 17 \cdot 5 = 85$

$3 \cdot 17 \cdot (17 \bmod 5) + 14 \cdot 5 \cdot (5^{-1} \bmod 17)$

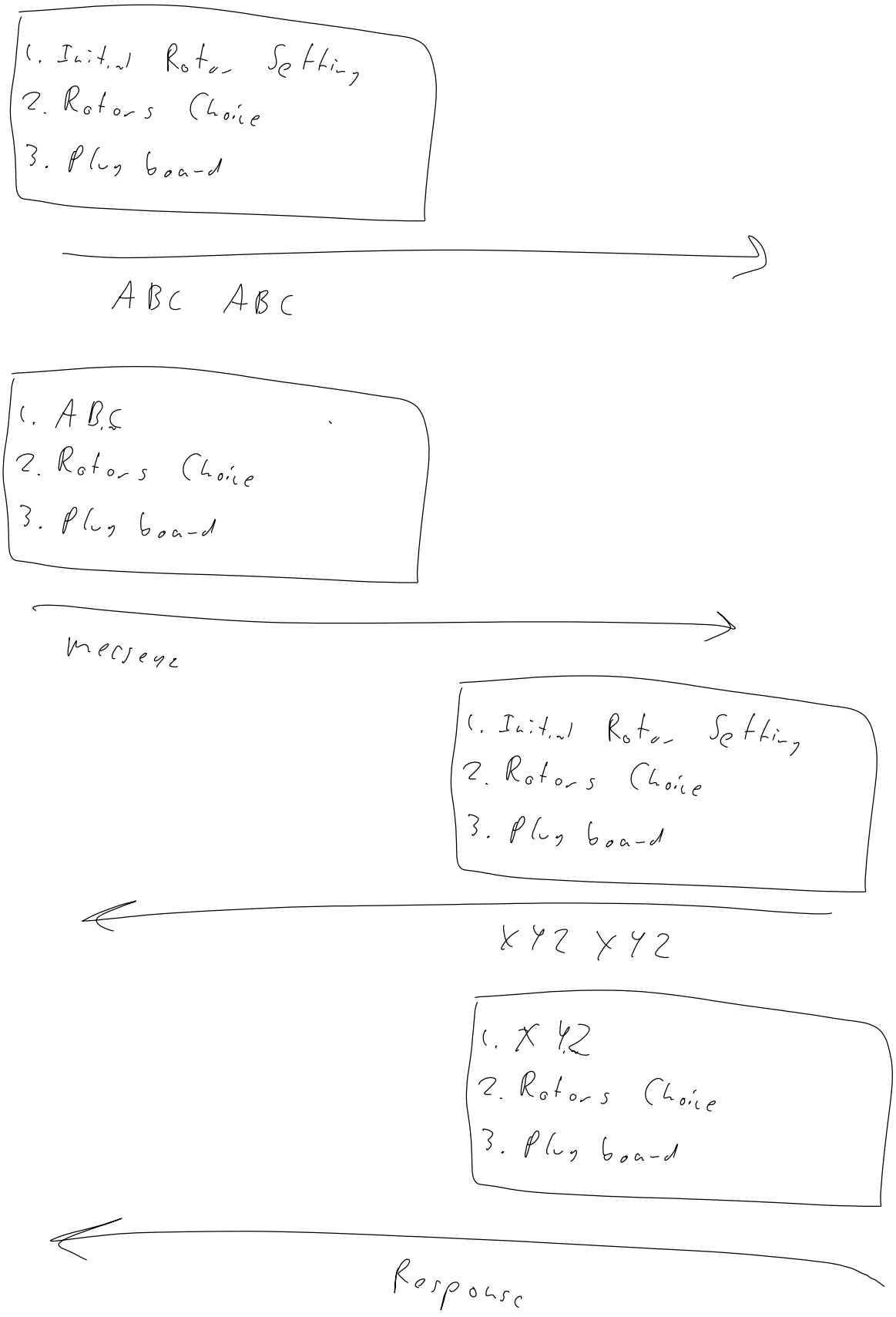
$3 \cdot 17 \cdot 3 + 14 \cdot 5 \cdot 7$

$= 153 + 490 = 643 \equiv 48 \pmod{85}$

Example: x ≡ 3 mod 5, & x ≡ 14 mod 17, & x ≡ 7 mod 11

Practice: x ≡ 3 mod 11, & x ≡ 2 mod 5, & x ≡ 6 mod 7

Wednesday, September 20, 2023 2:19 PM



CRT ⟶ 1 unique solution $< bd$.

$x \equiv a \mod b$

$x \equiv c \mod d$

$x \equiv e \mod f$

$x \equiv g \mod h$

$1, 2, 3, \ldots bd$

$x \equiv 3 \mod 5 \longrightarrow x \equiv 3 + k(5)$

$x \equiv 4 \mod 6$

$3, 8, 13, 18$

Guass' Algorithm, modular expnentiation

Thursday, September 7, 2023 4:19 PM

Announcements:

- Homework #4
  - Due Monday 18th
  - Should be 1 PDF file (applies to all HW from now on)
- Lectures 9 & 10 will be Async
  - Uploaded by class time
  - You are expected to have watched them by next Friday (possible quiz)

Gauss' Algorithm

- Example: $x \equiv 3 \bmod 5, x \equiv 14 \bmod 17$
- GCD(5,17) = 1
- Therefore 1 unique solution(s) up to $5 \cdot 17 = 85$
- $17^{-1} \bmod 5 = 3$
- $5^{-1} \bmod 17 = 7$

$$3 \cdot 17 (17^{-1} \bmod 5) + 14 \cdot 5 (5^{-1} \bmod 17) \pmod{17 \cdot 5}$$

$$3 \cdot 1 + 0 \pmod 5$$

$$0 + 14 \cdot 1 \pmod{17}$$

Example: $x \equiv 3 \bmod 5$, & $x \equiv 14 \bmod 17$, & $x \equiv 7 \bmod 11$

Given:

$(17*11)^{-1} \bmod 5 = 3$

$(5*11)^{-1} \bmod 17 = 13$

$(5*17)^{-1} \bmod 11 = 7$

$$3 \cdot 17 \cdot 11 \cdot ((17 \cdot 11)^{-1} \bmod 5) + 14 \cdot 5 \cdot 11 \cdot ((5 \cdot 11)^{-1} \bmod 17) + 7 \cdot 5 \cdot 17 \cdot ((5 \cdot 17)^{-1} \bmod 11) \pmod{}$$

$$3 \cdot 1 + 0 + 0 \equiv 3 \pmod{}$$

$$0 + 14 \cdot 1 + 0 \equiv 14 \pmod{}$$

$$6 + 0 + 7 \cdot 1 \equiv 2 \pmod{}$$

Practice: $x \equiv 3 \bmod 11$, & $x \equiv 2 \bmod 5$, & $x \equiv 6 \bmod 7$

$$3 \cdot 5 \cdot 7 \cdot ((5 \cdot 7)^{-1} \bmod 11) + 2 \cdot 7 \cdot 11 ((7 \cdot 11)^{-1} \bmod 5) + 6 \cdot 11 \cdot 5 \cdot ((5 \cdot 11)^{-1} \bmod 7)(\ldots$$

$$3 \cdot 5 \cdot 7 \cdot 6 + 2 \cdot 7 \cdot 11 \cdot 3 + 6 \cdot 11 \cdot 5 \cdot 6 \pmod{385}$$

Modular Exponentiation

$x^a \equiv ? \bmod n$

Example $3^a \bmod 11$

$x^2 = x^2$ ×4

$(x^2)^2 =$ ×8

$((x^2)^2)^2 =$ ×16

$(((x^2)^2)^2)^2 =$

2 in binary?

10

100

1000

10000

$3^2 \equiv 9$ $3^4 \equiv 4$ $3^8 \equiv 5$ $3^{16} \equiv 3$

$3^{32} \equiv$ $3^{64} \equiv$ $3^{128} \equiv$ $3^{256} \equiv$

$3^{512} \equiv$ $3^{1024} \equiv$ $3^{2048} \equiv$

$3^{563} \equiv ? \bmod 11$

$563_2 =$ 1 0 0 0 1 1 0 0 1 1

$512 + 0 + 0 + 0 + 32 + 16 + 0 + 0 + 2 + 1$

1000110011

563 − 512 = 51; 51 − 32 = 19; 19 − 16 = 3

$3^{563} \equiv (3^{512})(3^{32})(3^{16})(3^2)3^1 \pmod{11}$

$\equiv 9 \cdot 9 \cdot 3 \cdot 9 \cdot 3 \equiv 3^8 \equiv 5$

Why is this useful?

Take a look at my spreadsheet

Practice

$5^{1790} \bmod 7 =$ 4

$5^{1876} \bmod 7 =$ 2

$5^{1915} \bmod 7 =$ 5

$5^{2017} \bmod 7 =$ 5

$5^{2025} \bmod 7 =$ 6

Fermat's and Euler's Theorems

Friday, September 8, 2023 3:10 PM

Objectives:

- Fermat's Little Theorem
- Euler's Totient Function
- Euler's Theorem

Fermat's Little Theorem:

If p is a prime and p does not divide a, then:

Proof: $a^{p-1} \equiv 1 \pmod{p}$

$S = 1, 2, 3 \ldots p-1$ $\quad F(S) \to S$

Let $F(x) \equiv ax \bmod p$

(1) $F(x) \not\equiv 0$ ✓ (2) if and only if $x \equiv y$ then $F(x) = F(y)$ ✓

Assume $F(x) \equiv 0 \to ax \equiv 0 \pmod{p}$ $\quad x \equiv 0 \pmod{p}$

If $x, y \in S$ with $F(x) = F(y) \to ax \equiv ay \pmod{p}$ $\quad x \equiv y \pmod{p}$

Assume $x \not\equiv y$ $\quad ax \not\equiv ay$ $\quad F(x) \not\equiv F(y)$

$F(S) \to S$

$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv (p-1)! \equiv F(1) \cdot F(2) \cdot F(3) \ldots F(p-1)$

$\equiv a \cdot 1 \cdot a \cdot 2 \cdot a \cdot 3 \ldots a(p-1) \equiv a^{p-1} \, 1 \cdot 2 \cdot 3 \ldots$

$(p-1)! \equiv a^{p-1} (p-1)!$

$1 \equiv a^{p-1} \pmod{p}$

Example:

$2^{103} \equiv ?$ mod 11

$a = 2 \quad p = 11 \quad p-1 = 10 \quad 1 \equiv 2^{10} \pmod{11}$

$2^{103} \equiv (2^{10})^{10} \, 2^3 \equiv (1)^{10} \, 2^3 \equiv \boxed{8 \pmod{11}}$

$3^{132} \equiv ?$ mod 13

$a = 3 \quad p = 13 \quad p-1 = 12$

$3^{12} \equiv 1 \pmod{13}$

$3^{132} = (3^{12})^{10} \cdot 3^{12} \equiv 1^{10} \cdot 1 \equiv 1 \pmod{13}$

$\phi(10) = 20 \cdot (1 - \frac{1}{2})(1 - \frac{1}{5})$

Euler's Totient Function

$\phi(n) = n \cdot \prod (1 - \frac{1}{p})$ for all distinct $p \mid n$

Why does it matter?

Example:

n = 10

1, 2, 3, 4, 5, 6, 7, 8, 9 $\quad GCD(a, n) = 1 \quad 0 < a < 1$

$\phi(10) = 10 (1 - \frac{1}{5})(1 - \frac{1}{2}) = 10 \cdot \frac{4}{5} \cdot \frac{1}{2} = 4$

n = 9

1, 2, 3, 4, 5, 6, 7, 8

$\phi(9) = 9 (1 - \frac{1}{3}) = 9 \cdot \frac{2}{3} = 6$

General Case:

$\phi(n) = n \prod (1 - \frac{1}{p})$

Special Cases:

$\Phi(p) = p(1 - \frac{1}{p}) = p - 1$

$\Phi(p^r) = p^r (1 - \frac{1}{p})$

n = pq -> $\Phi(pq) = (p-1)(q-1)$

$n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) = pq\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)$

$(p-1)(q-1)$

Example

$\Phi(10) = (5-1)(2-1) = 4$

$\Phi(9) = 3^2\left(1-\frac{1}{3}\right) = (3^2)\frac{2}{3} = 6$

Keep in mind: you must know the factorization of n to compute the totient

Euler's Theorem

$$a^{\phi(n)} \equiv 1 \mod n$$

What if a is prime? (n = p)

$$a^{\phi(p)} \equiv a^{p-1} \equiv 1 \mod p$$

Euler's Theorem and Primative Roots

Friday, September 8, 2023 3:13 PM

Euler's Theorem

If GCD(a,n) = 1 then:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

$$\phi(n) = n \cdot \prod \left(1 - \frac{1}{p}\right)$$

What if n is prime? (n = p)

$$a^{p-1} \equiv 1 \pmod{p}$$

Example

What are the last three digits of 7^{803}?

$$\pmod{1000}$$

$$10 \cdot 10 \cdot 10 = 5 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \cdot 2$$

$$\phi(1000) = (5 \cdot 2)^3 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 5^3 \cdot 2^3 \left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 5^2 \cdot 2^2 \cdot 4 = 400$$

$$7^{400} \equiv 1 \pmod{1000}$$

$$7^{803} \equiv 7^{400}\, 7^{400}\, 7^3 \equiv 7^3 \equiv 49 \cdot 7 \equiv \boxed{343}$$

What are the last two digits of 3^{963}?

$$\pmod{100}$$

$$\phi(100) = (5 \cdot 2)^2 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 5^2 \cdot 2^2 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

$$3^{40} \equiv 1 \pmod{100}$$

$$3^{963} \equiv (3^{40})^{10} (3^{40})^{10}\, 3^{163} \equiv 3^{160}\, 3^3 \equiv (3^{40})^4\, 3^3 \equiv \boxed{27}$$

If you wanted to check your work by hand what would you do?

Primitive Roots (or generators)

Look at powers mod 7

	$1^1 \equiv 2$	$1^2 \equiv 4$	$1^3 \equiv 1$	$1^4 \equiv 2$	$1^5 \equiv 4$	$1^6 \equiv 1$
○	$2^1 \equiv 3$	$2^2 \equiv 2$	$2^3 \equiv 6$	$2^4 \equiv 4$	$2^5 \equiv 5$	$2^6 \equiv 1$
	$3^1 \equiv 4$	$3^2 \equiv 2$	$3^3 \equiv 1$	$3^4 \equiv 4$	$3^5 \equiv 2$	$3^6 \equiv 1$
(5)	$4^1 \equiv$	$4^2 \equiv$	$4^3 \equiv$	$4^4 \equiv$	$4^5 \equiv$	$4^6 \equiv$

1 ✓
2 ✓
3 ✓
4 ✓
5 ✓
6 ✓

Number of primitive roots of a prime p = Φ(p-1)

How many primitive roots does 7 have? $\phi(6) = 6\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 2 \cdot 3\left(\frac{1}{2}\right)\left(\frac{2}{3}\right) = 2$

How to show that a given g is a generator or primitive root mod p:

$g = 1 \quad p = 7 \quad 1^{7-1} \equiv 1^6 \equiv 1$

$g = 3 \quad p = 7 \quad 3^{7-1} \equiv 3^6 \equiv 1$

Verify that g^{p-1} is the **first** power of g that is congruent to 1 mod p

How to show that a given g is not a generator of mod p:

1 Factor p-1

2 Divide p-1 by each of its factors

3 Raise g to these results

4 If any turn out to be congruent to 1 mod p, g is NOT a primitive root

Give an example with p = 13

How many primative roots does 13 have?

$\phi(12) = 2 \cdot 2 \cdot 3\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 2 \cdot 2 \cdot 3\left(\frac{1}{2}\right)\left(\frac{2}{3}\right) = 4$

What are they? (use Excel)

2, 6, 7, 11

Practice:

How many primitive roots does 6 have?

0

How many primative roots does 17 have?

$\phi(16) = 2^4\left(1-\frac{1}{2}\right) = 8$

What are they? (use Excel)

3, 5, 6, 7, 10, 11, 12, 14

DES (Data Encryption Standard)

Thursday, September 14, 2023 5:39 PM

Announcements

- HW #3 went well:
  - 4 – 2 * 3 (mod 5)
  - Shift Cipher Key = 3
- INL update
- Course roadmap
- Objective for today: learn DES

1973 NBS (National Bureau of Standards) publishes request for encryption algorithm

1974 second request goes out, IBM submits Lucifer

- Designed by Horst Feistel
- Team brought into NSA and together they produce DES – NSA shortened the key to 56 bits, reduced block size to 64 bits, and strengthened the algorithm against differential cryptanalysis (known only to IBM and NSA)

1975 DES published in Federal Register for comment

1976 DES approved as a standard

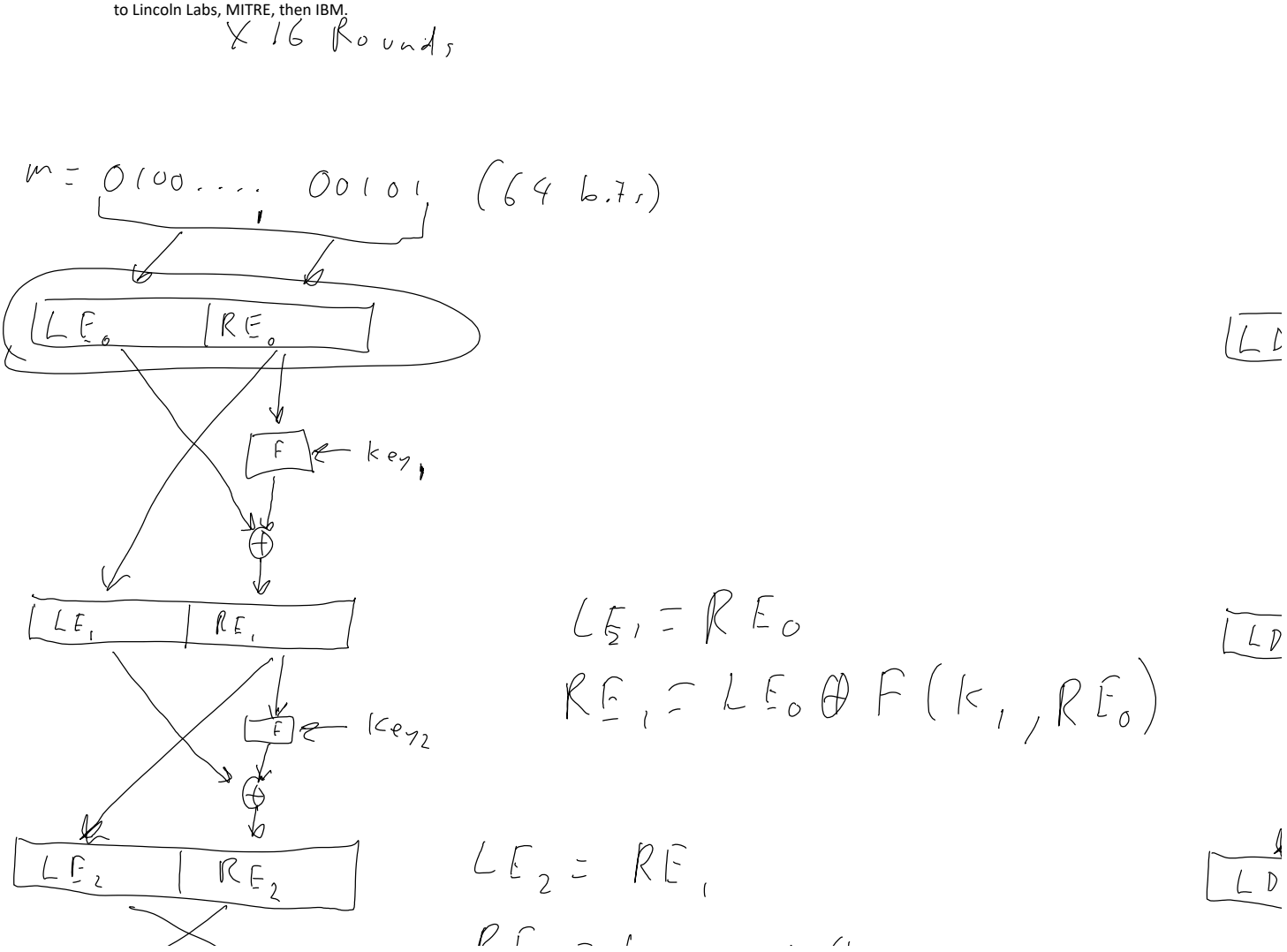
1977 DES published as FIPS (Federal Information Processing Standard) PUB 46

1983, 1988, 1993, 1999 Reaffirmed as a standard
(Triple DES, single DES legacy only)

2005 Withdrawn as a standard

3 components of DES:

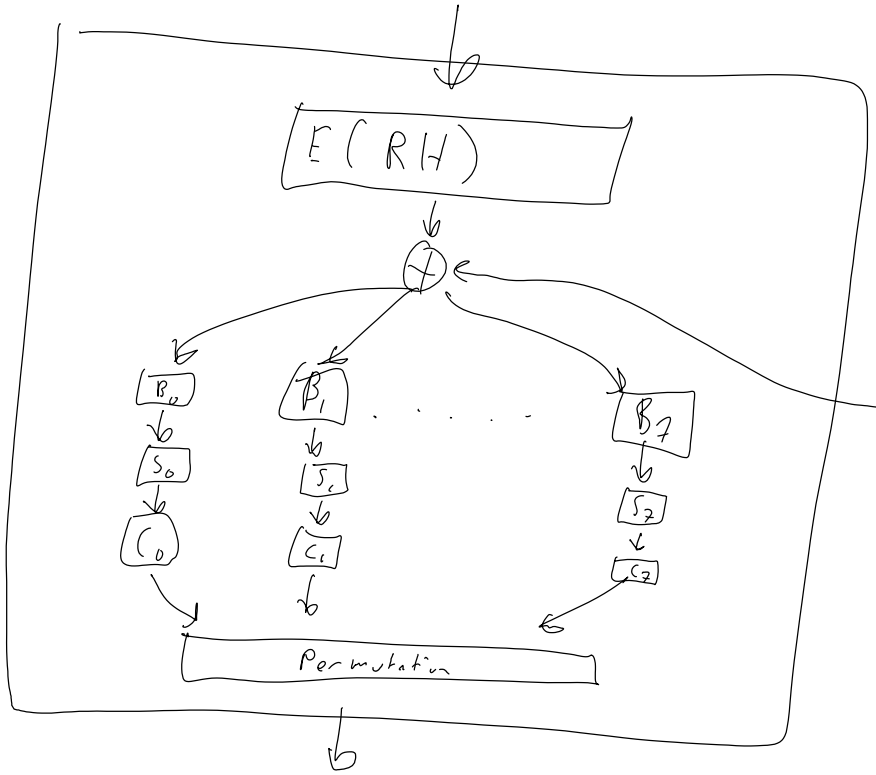
- Feistel Algorythm
  - Horst Feistel – Born in Berlin in 1915, moved to US in 1934. Arrested at beginning of WWII. Made a citizen on 31 Jan 1944. Worked on IFF systems at AFCRC, then went to Lincoln Labs, MITRE, then IBM.



$RE_2 = LE_1 \oplus F(K_2, RE_1)$

$RE_2 \mid LE_2$ = Ciphertext

DES function

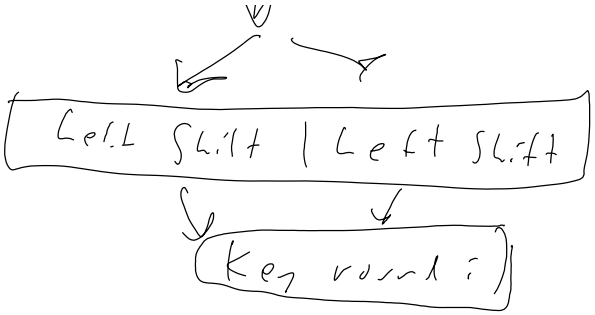


Key generation

Key (64 bit)

Permutation

(56 bit)



(48 bits)

Modes of Operation (Powerpoint)

- ECB is bad
- CBC fixes its problems
- CFB is faster than CBC because only encryption is done and only part of the block needs to be encrypted before feeding into the next block
- CTR and OFB are stream ciphers (faster)
- CTR is better than OFB because OFB IVs are more likely to repeat.

DES 2nd Lecture

Monday, September 18, 2023 11:43 AM

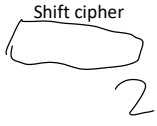
Objectives:

Go over HW#1 - examples of good/bad code

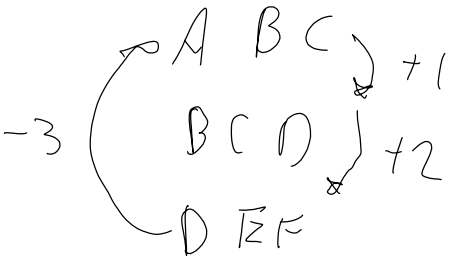
Talk about Triple DES

Double encryption is sometimes ineffective

Shift cipher



26



Double shift cipher

26

Triple shift cipher

26

Viginere cipher (key length 4)

[a, b, c, d] 26^4

Double Viginere cipher (key length 4,4)

26^4

Double Viginere cipher (key length 3,4)

26^{12}

Security vs. Key length

Made up security protocol:

Video

DES = 56 bit security

AES = 128 - 256 bit security

Double DES

57 bits

$E_{k_2}(E_{k_1}(m))$

Triple DES

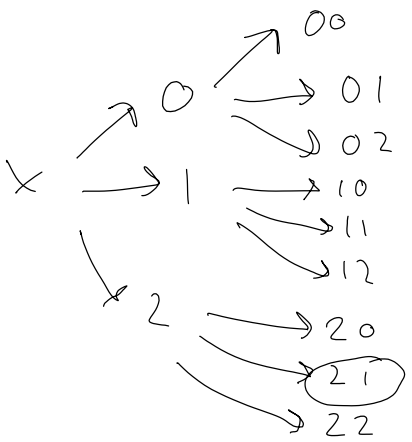
112 bits

$E_{k_3}(E_{k_2}(E_{k_1}(m)))$

Meet-in-the-Middle Attacks

$$E_{k_1}(D_{k_2}(E_{k_1}(m)))$$

$X \rightarrow 0, 1, 2 \rightarrow 9$ possibilities



Eve

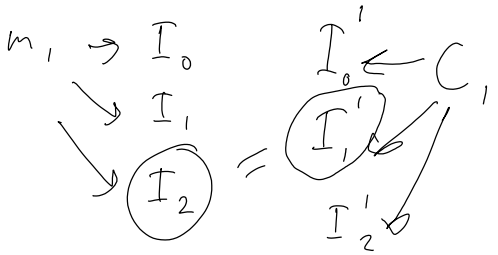
m_0

~~key~~

C_1

m_1

$$m_1 \xrightarrow{k_1} I \xrightarrow{k_2} C_1$$



Asymetric Intro - RSA

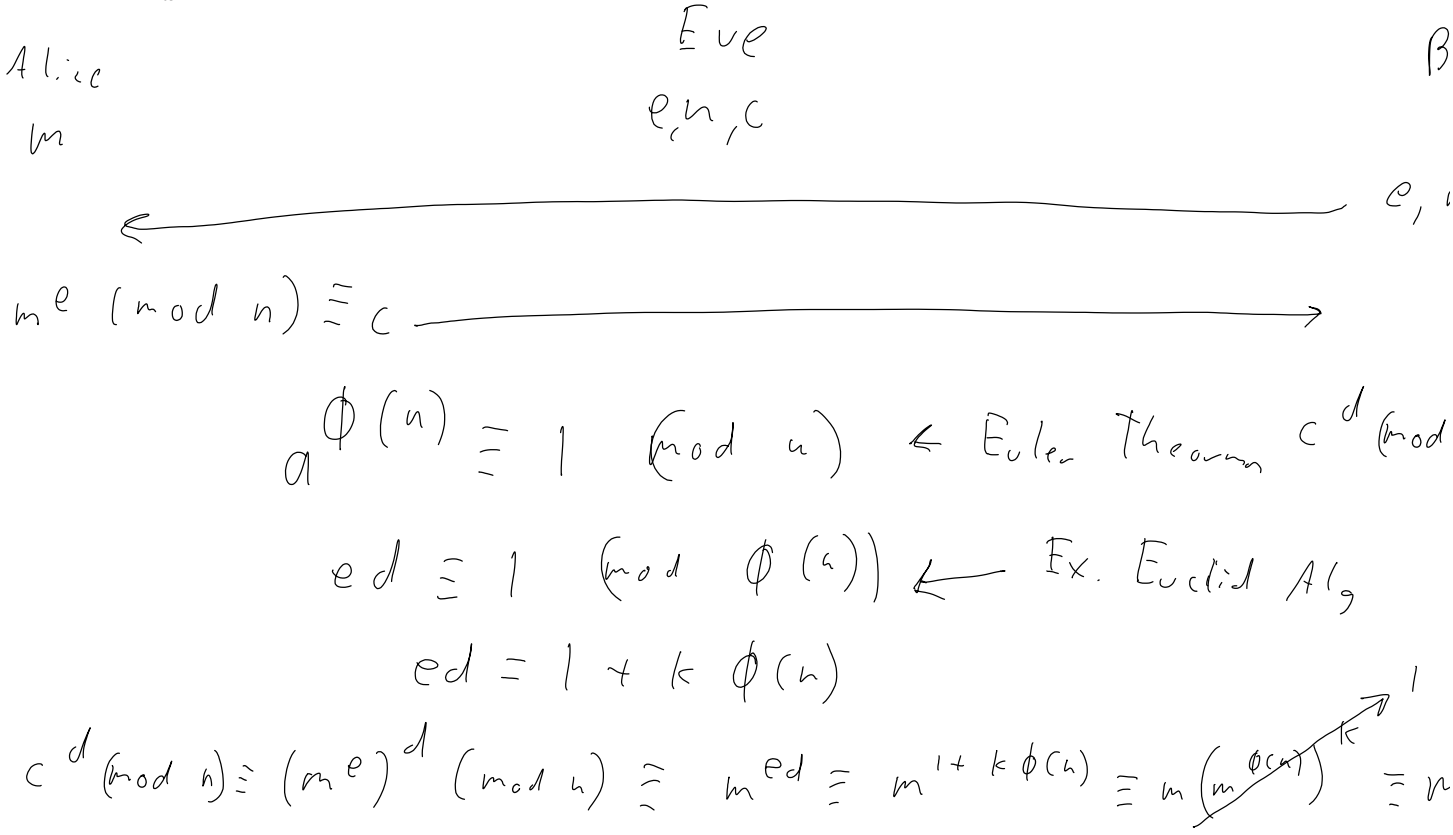
Friday, September 22, 2023 4:49 PM

Onjectives:

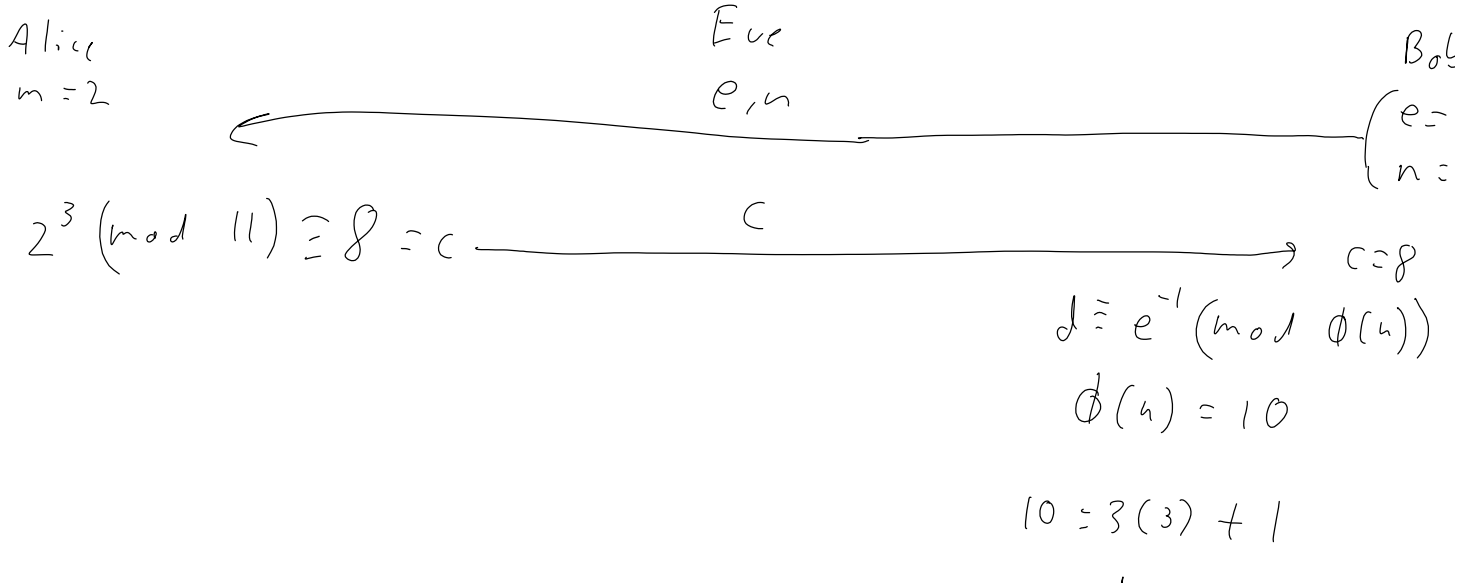
- Intro
- Symmetric vs Asymmetric
- RSA_{lite}
- RSA
- RSA Implementation

Symmetric vs Asymmetric

Example of RSA_{lite} (with variables)



RSA_{lite} Example e = 3, n = 11 and m=2



$d \equiv -3 \equiv 7 \pmod{10}$

$8^7 \pmod{11} \equiv 2$

$c^d \pmod{n} = m$

Practice using RSA_{lite}!

e=3 and n=17

C = 5

C = 13

C = 6

C = 12

C = 3

C = 2

C = 15

C = 14

$c = 6 \quad e = 3 \quad n = 17 \qquad \phi(17) = 16$

$d \equiv 3^{-1} \pmod{16} \rightarrow 16 = 3(5) + 1$

$d \equiv -5 \bmod 16$

$6^{11} \bmod 17$

$(6^2 \cdot 6^2 \cdot 6^2 \cdot 6^2 \cdot 6^2 \cdot 6^1) \bmod$

$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 6 = 1$

What is Φ(n)? $\phi(n) = n \prod_{i|n} \left(1 - \frac{1}{p}\right)$

Can Eve calculate Φ(n)?

What information is needed to calculate Φ(n)?

Full example of RSA (p=17, q=19, m=2)

$n = p \cdot q = 323$

$\phi(n) = 16 \cdot 18 = 288$

$? = 3^{-1} \pmod{288} \quad GCD(3, 288) = 96 \quad e \neq 3$

$e = 5$

$5^{-1} \pmod{288}$

$288 = 5(57) + 3$ $\quad 288(1)$

$5 = 3(1) + 2$ $\quad 288(-1)$

$3 = 2(1) + 1$ $\quad 288(2)$

$d \equiv -115 \equiv 173$

$m = 2$

$2^{5} \pmod{323} \equiv 32 = C$

$32^{173} \pmod{288} \equiv 2$

Practice (e=5,p=7,q=13)

C = 2

C = 3

C = 4

C = 5

C = 6

C = 7

C = 8

C = 9

Implementation

RSA Attacks

Friday, September 22, 2023 4:48 PM

RSA – Rivest, Shamir, and Adleman 1977, Clifford Cocks 1973 (GCHQ)

Review RSA (e = 155, p = 23, q = 19)

C = 101 423
C = 102 125
C = 103 126
C = 104 35
C = 105 179
C = 106 83

$n = pq$

$23(19) = 437$

$\phi(n) = 22 \cdot 18 = 396$

$155^{-1} \pmod{396} =$

$C^{23} \pmod{437}$

$x^{\phi(n)} \equiv 1 \pmod{n}$

$ed \equiv 1 \pmod{\phi(n)}$

$m^e \equiv c \pmod{n}$

$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{1 + k\phi(n)} \equiv m$

Attacks on RSA

Mind your p's and q's:

If m/4 of your p or q is know -> bad

Poorly chosen p and q

$p, q = x \pm 1$

$\sqrt{n} \approx x$

Example p =11, q = 13

$\sqrt{143} = 11.9\ldots \approx 12$

Practice with n = 5183, e = 11. What is m?

C = 611 2017
C = 578 1790
C = 813 1126
C = 2885 2025
1915

$p = 71$

$q = 73$

C = 1928

$$\phi(n) = 5040 = 70 \cdot 72$$

$$d \equiv 11^{-1} \pmod{5040} = 2291$$

$$C^{2291} \pmod{5183} \equiv m$$

Chosen Ciphertext attack

Theory

given: C + mechanism for decrypting

$$C \cdot 2^e \equiv X$$

$$x^d \pmod n \equiv (C \cdot 2^e)^d \equiv c^d \cdot 2^{ed} \equiv c^d \cdot 2$$

$$c^d \equiv m \pmod n$$

Example with e = 155, n=437, c = 102

$$x = 102 \cdot 2^{155} \equiv 181 \pmod n$$

$$181^{23} \pmod{437} \equiv \frac{250}{2} = 125$$

Low exponent attacks

Coppersmith attack

Don't pick e = 3

~~E = 65537~~ popular choice.

How to compute?

Wiener's Attack $((m^2)^2)^2 \cdots \cdot m$

Only works if d is very small:

Math:

$$d < \frac{1}{3} n^{1/4}$$

(x - p) (x - q) =

N - Φ(n) +1 = $x^2 - (p+q)x + n$

$pq - (p-1)(q-1) + 1 = pq - pq + p + q - 1 + 1$

$= p + q$

$$x^2 + (-n + \phi(n) - 1)x + n$$

$$\Phi(n) = \frac{ed - 1}{k}$$

$$ed \equiv 1 \pmod{\phi(n)} \qquad ed = 1 + k\phi(n)$$

Demonstrate little d attack (e = 4811, n = 7387)

$$\frac{e}{n} = \frac{4811}{7387} = 0 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{9 + \cfrac{1}{4}}}}}}}}}}$$

$[0; 1, 1, 1, 6, 1, 1, 4, 9, 4]$

	0	1	0	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{2}{3}$
1	0	1	1			

$\frac{k}{d} \stackrel{?}{=} \frac{1}{1}$ X

$\frac{1}{1 + \frac{1}{1}} = \frac{1}{2}$ X

$\frac{1}{1 + \frac{1}{1 + \frac{1}{1}}} = \frac{2}{3} \stackrel{?}{=} \frac{k}{d}$ $\quad \phi(n) \stackrel{?}{=} \frac{ed - 1}{k} = \frac{4811 \cdot 3 - 1}{2} = 7216$

$Ax^2 + Bx + C$

$x^2 + (-n + \phi(n) - 1)x + 1$

$A = 1$

$B = -7387 + 7216 - 1 = -172$

$C = 7387$

$$\frac{-B \pm \sqrt{B^2 - 4AC}}{2A}$$

$$\frac{172 \pm \sqrt{36}}{2}$$

$$\frac{172 \pm 6}{2}$$ $\boxed{x = 83, 89}$

$ed \equiv 1 \pmod{\phi(n)}$ $\quad \phi(n) = (p-1)(q-1)$

Practice with e = 60267, n = 91027

$[0; 1, 1, 1, 23, 1, 1, 4 \ldots]$

$\frac{0}{1}$ X

$\frac{1}{1}$ X

$\boxed{\phi(n) = \frac{ed - 1}{k}}$

$\frac{1}{2} \times$

$\frac{2}{3} \stackrel{?}{=}$ $\qquad \phi(n) \stackrel{?}{=} 90400$

$$0 = x^2 + (-n + \phi(n) - 1)x + n$$

$$0 = Ax^2 + Bx + C$$

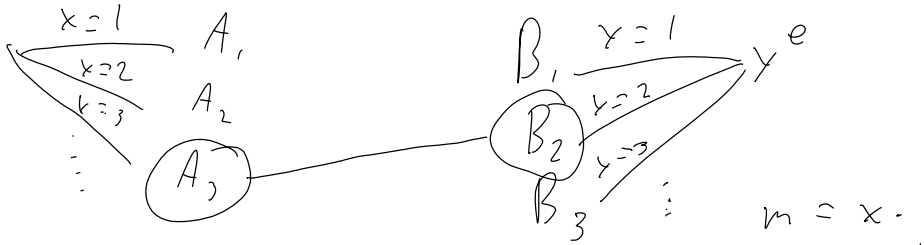
$$-628 = \begin{cases} A = 1 \\ B = -n + \phi(n) - 1 \\ C = n \end{cases}$$

$$\frac{-B \pm \sqrt{B^2 - 4}}{2A}$$

$$\begin{cases} p = 227 \\ q = 401 \end{cases}$$

Short Plaintext attack Demo

$c \cdot x^{-e} \pmod n$



Example with e = 3, n = 1927, c = 1728

$1728 \cdot x^{-3} \pmod{1927}$

x^{-1}	x	
	$x=1$	1728
-963	$x=2$	241
1285	$x=3$	64
	$x=4$	

$y^3 \pmod{1927}$	y
1	$y=1$
8	$y=$
27	$y=$
64	$y=$

$1927 = 2(963) + 1$

$x^{-3} = (x^{-1})^3$ $1927 = 3(642) + 1$

$3 \cdot 4 = m = 12$

Practice with e = 3, n = 2491, c = 216

$2^{-1} \pmod{2491}$

x	x^{-1}	$x^{-e}(c)$
1	1	
2	1246	27
3		
4		

$2491 = 2 \cdot 1245 + 1$

~~$2 = 1 \cdot 2 + 0$~~

$2491 - 2($ $= 1$

y^3	y
1	1
8	2
27	3
64	4

$2 \cdot 3 = \boxed{6}$

$m^e < n$

$e\sqrt{c} = m$

Primality Testing

Thursday, September 28, 2023 12:34 PM

Why is this subject important?

You will code up the Miller-Rabin in PEX3

Miller-Rabin Algorithm

Basic Principle for Factoring:

If n is an integer, and you can find x and y s.t. $x^2 \equiv y^2 \bmod n$ and $x \neq \pm y \bmod n$

Then GCD(x-y,n) is a non-trivial factor of n (treasure pair)

Why is this more efficient than brute force?

Different type of algorithms:

Deterministic

Input n (is n prime?) ->

Probabilistic

Input n and witness (is n prime?) ->

What have all the algorithms in this class been so far?

Is probabilistic better?

Remember Fermat's Little Theorm

Recall, if a random integer $1 < a < n-1$, then $a^{n-1} \neq 1 \bmod n$ then n is composite. If $a^{n-1} \equiv 1 \bmod n$ then n is probably prime.

We can perform modular exponentiation by successive squaring. If we are careful in doing this we can get a stronger result.

Step 1: Pick n

Step 2: Find odd m such that $n - 1 = 2^k m$

How do you express n-1 as $2^k m$?

Repeatedly divide by 2 until you get an odd remainder.

Step 3: Pick a random witness a [2,n-2]

Step 4: Compute $b_0 \equiv a^m \bmod n$

If b0 ≡ ±1 then stop and declare n probably prime.

Why?

Step 4: Otherwise form $b_1 \equiv b_0^2$

If b1 ≡ 1 then n is composite

What is the factor?

If $b_1 \equiv -1$ then stop and declare n is probably prime

Step 5: Otherwise form $b_2 \equiv b_1^2$

If b2 ≡ 1 then n is composite

If b2 ≡ -1 then stop and declare n is probably prime

Step 6: Continue until stopping or reaching b_{k-1}.

If bk-1 ≠ -1 mod n, then n is composite.

	Stop – Probably Prime	Stop n composite	Continue computing b_k
$b_0 \equiv a^m \equiv \pm 1$	$b_0 \equiv \pm 1$	-----	otherwise
$b_1 \equiv b_0^2$	$b_1 \equiv -1$	$b_1 \equiv 1$	otherwise
$b_2 \equiv b_1^2$	$b_2 \equiv -1$	$b_2 \equiv 1$	otherwise
…			
$b_{k-1} \equiv b_{k-2}^2$	$b_{k-1} \equiv -1$	$b_{k-1} \neq -1$	-----

Examples n = 21 with witness 2

$n-1 = 2^k m$ $\quad 21-1 = 2^2 \cdot 5$ ✓

$21-1 = \frac{20}{2} = \frac{10}{2} = 5 = m$ $\quad k = 2$

$b_0 \equiv 2^5 \pmod{21} \equiv 11$ $\quad k=2$

$b_1 \equiv 11^2 \pmod{21} = 16$ $\quad 2-1 = 1$

Example n = 17 with witness 2

$n = 17$

$n-1 = 16$ $\quad \frac{16}{2} = \frac{8}{2} = \frac{4}{2} = \frac{2}{2} = 1$ $\quad m = 1$ $\quad k = 4$ $\quad 2^4 \cdot 1 = 16$

$2^1 \equiv b_0 \pmod{17}$

$2^2 \equiv b_1 \pmod{17} \equiv 4$

$b_2 \equiv 4^2 \equiv 16 \pmod{17} \equiv -1$

Probably Prime

Odds that n is prime is 4^{-w}, where w is the number of witnesses.

You try with 25

Use witnesses 5, 6, 7, 8, 9,10

$m = 3$

$k = 3$

$b_0 \equiv 2^3 \pmod{25} \equiv 18$

$b_1 \equiv b_0^2 \equiv -1$

Factoring

Thursday, September 28, 2023 9:10 PM

Four methods for factoring n

1. Search all primes less than or equal to the squareroot of n
   Is this a efficent stratagy?
2. Fermat Factorization
   a. N + x*x = y
      i. Start with x = 1 and increment until y is a square
      ii. Then sqrt(y) +/- x = root
   Example: n = 16

$16 + 1^2 = 17$ X

$16 + 2^2 = 20$ X

$16 + 3^2 = 25$

$\sqrt{25} = 5$

$5 - 3 = 2$

Practice: n = 20

$x = 4 \quad 20 + 4^2 = 36 \quad 6 \pm 4 = 2, 10$

Practice on board: n = 5

$5 + 1^2 = 6$

$5 + 2^2 = 9$

$\sqrt{9} = 3$

$3 + 2 = 5$

$3 - 2 = 1$

1. p - 1 factoring meathod
   a. Choose a and B
      (a = 2 and B depends on how long you want to keep trying)
   b. Let $b_1 \equiv a \pmod n$
   c. While i < B:
      i. $b_i \equiv (b_{i-1})^i \pmod n$
   d. Ultimately $b \equiv a^{B!} \pmod n$
   e. Find d = gcd(b-1, n)
   f. If 1 < d < n, then d | n
   Example: n = 18, a =2 , B = 5

$b_i = (b_{i-1})^i$

$b_1 = 2 \pmod{18}$

$b_2 = b_1^2 = 2^2 = 4 \pmod{18}$

$b_3 = b_2^3 = 4^3 = 10 \pmod{18}$

$b_4 = b_3^4 = 10^4 = 10 \pmod{18}$

$b_5 = b_4^5 = 10^5 = 10 \pmod{18}$

$b_5 = (b_4)^5 = ((b_3)^4)^5 = b_1$

$b-1 = 9 \quad d = \gcd(9, 18$

Practice: n = 20, a =2, B =5

$b_1 = 2$

$b_2 = 4$

$b_3 = 4$

$\gcd(15, 20) = 5$

$5^4 = 16$

$5^5 = 16^5 = 16$

4. Modern Methods

All based off of the idea:

If $x^2 \equiv y^2 \pmod n$ and not $x \equiv +/- y \pmod n$:

Then GCD(x - y, n) = root

These pairs are called treasure pairs

Is 1 and 26 a treasure pair mod 25? X

Is 5 and 10 a treasure pair mod 25? ✓

Is 1 and 24 a treasure pair mod 25? X

Is 5 and 15 a treasure pair mod 25? ✓

Is 10 and 15 a treasure pair mod 25? X

Practice: Find all treasure pairs <20 for n=35

(1) $x, y \quad x^2 \equiv y^2 \pmod n$

(2) $x \not\equiv \pm y \pmod n$

Discrete Logarithms, Diffe-Hellman, ElGamal

Wednesday, October 4, 2023 10:20 AM

Factoring is the hard problem for RSA. Other hard problems exist.

For example $a^b = c$.

Case 1 $a^b = x$, e.g. $3^5 = x$ ->

Case 2 $x^b = c$, e.g. $x^5 = 243$, $x = 3$->

Case 3 $a^x = c$, e.g. $3^x = 243$ $x = \log_3(243) = 5$ ->

Let's examine these cases mod 17

$3^5 \equiv x \pmod{17}$ ->

$x^5 \equiv 5 \pmod{17}$ ->

$3^x \equiv 5 \pmod{17}$ ->

What is $\log_2(8) \bmod 17$? Since $2^3 \equiv 8$, $\log_2(8) \equiv 3$.

But $2^{11} \equiv 8 \pmod{17}$ So what about 11?

But wait! $\log_4(5) \equiv$ DNE (mod 17)

Discrete logs guarenteed if:

1. Base is a
2. Modulus is a

What went wrong with $\log_4(5) \equiv$ DNE (mod 17)

Discrete Log Problem

Given a, b, n it is believed to be hard to find x in $a^x \equiv b \bmod n$.

Why do cryptographers like hard problems?

What is RSAs "hard problem"?

Diffie-Hellman Key Exchange uses discrete logs

Diffe-Hellman

Step 1. In the clear – Alice and Bob agree on a large prime p and a generator g (primitive root)

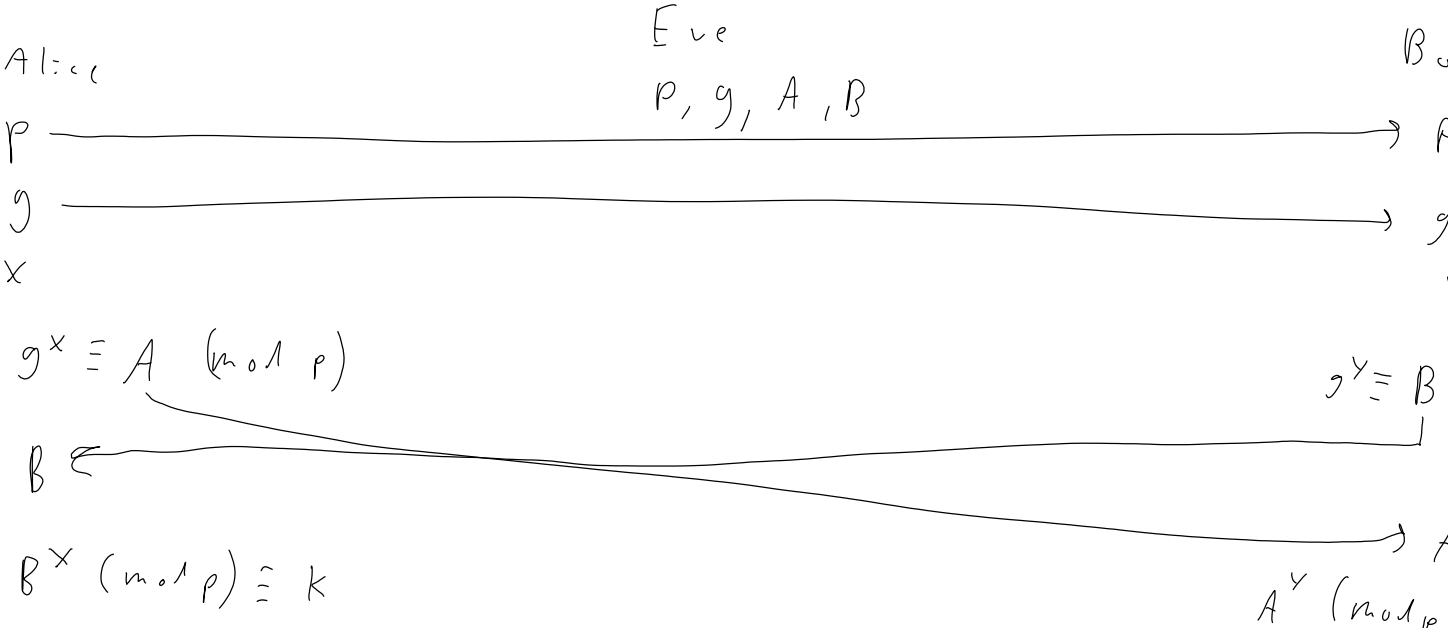
Step 2. In secret - Alice and Bob pick secret numbers x and y between 1 and p-2 inclusive

Step 3. Alice sends $g^x \bmod p$ to Bob and Bob sends $g^y \bmod p$ to Alice.

Step 4. They each compute the shared key K. $K = g^{xy} \bmod p$. Alice computes K by raising $(g^y)^x = g^{xy}$ mod and Bob computes K by raising $(g^x)^y \bmod p$.

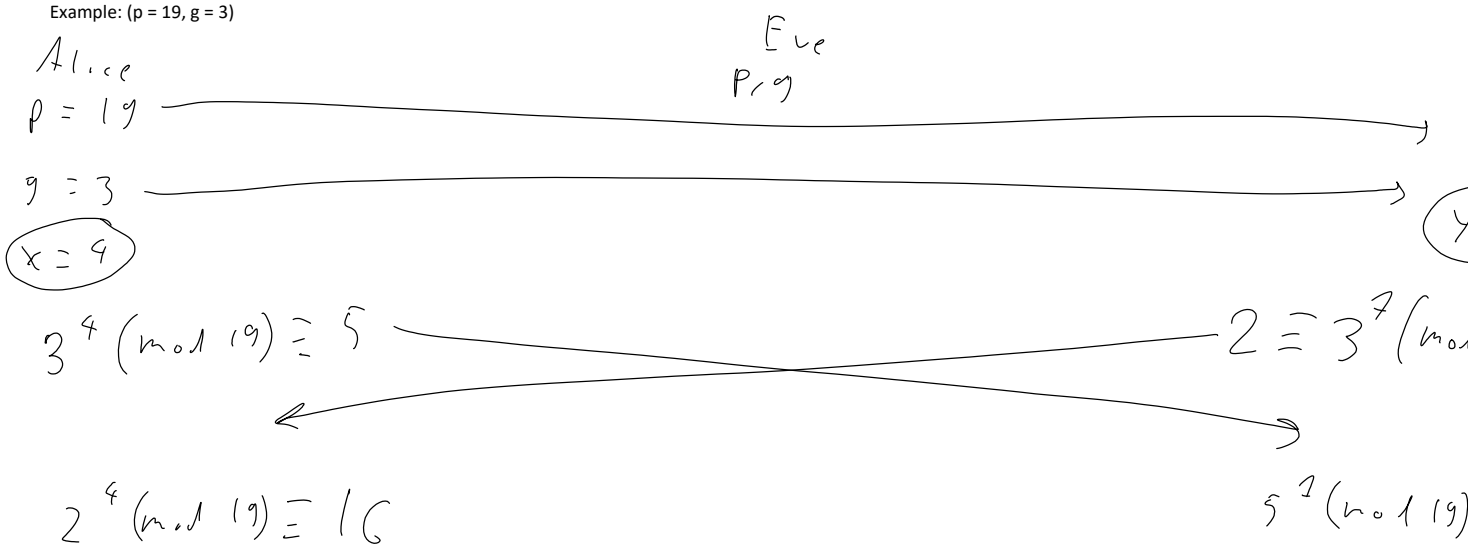
Step 5. Use some prearranged piece of K as their key (e.g. middle 56 bits for a DES key)

Example with letters:



$$k \pmod p \equiv \beta^x \equiv g^{yx} \equiv g^{xy} \equiv A^y \equiv k$$

Example: (p = 19, g = 3)



You try. Use (p = 11, g = 8)

Why does ElGamal exist?

(popularized because of antipathy toward the RSA patents)

RSA's hard problem is (factorization)

ElGamal's hard problem is (discrete logs)

Bob wants to send a message m to Alice securely. Alice chooses a large prime p and primitive root α. Alice also chooses a secret a and computes $\beta \equiv \alpha^a \bmod p$. Assume $0 \le m < p$. Otherwise break it into less than p sized chunks. (p, α, β) is published as Alice's public key.

Bob does:

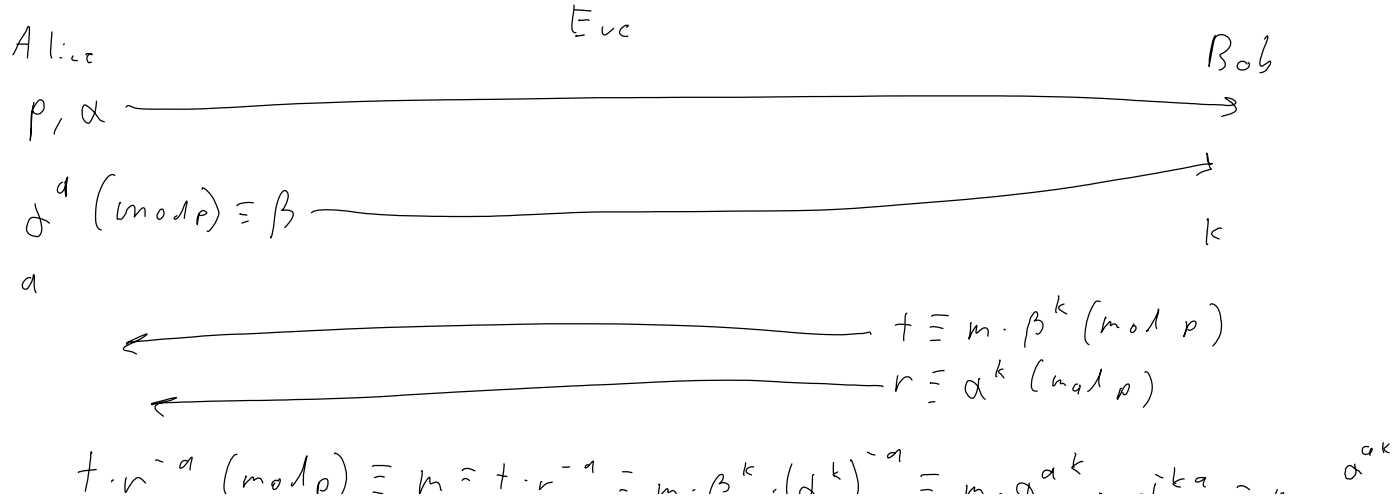
1. Downloads (p, α, β)
2. Chooses a secret random integer k and computes $r \equiv \alpha^k \bmod p$.
3. Computes $t \equiv \beta^k m \bmod p$
4. Sends the pair (r,t) to Alice

Alice decrypts:

5. $tr^{-a} \equiv m \bmod p$

Difficulty of computing discrete logs protects value of a.

It's hard to get k from r since this is also a discrete log problem. BUT if Eve gets k she can compute m from $t\beta^{-k} \equiv m \bmod p$.



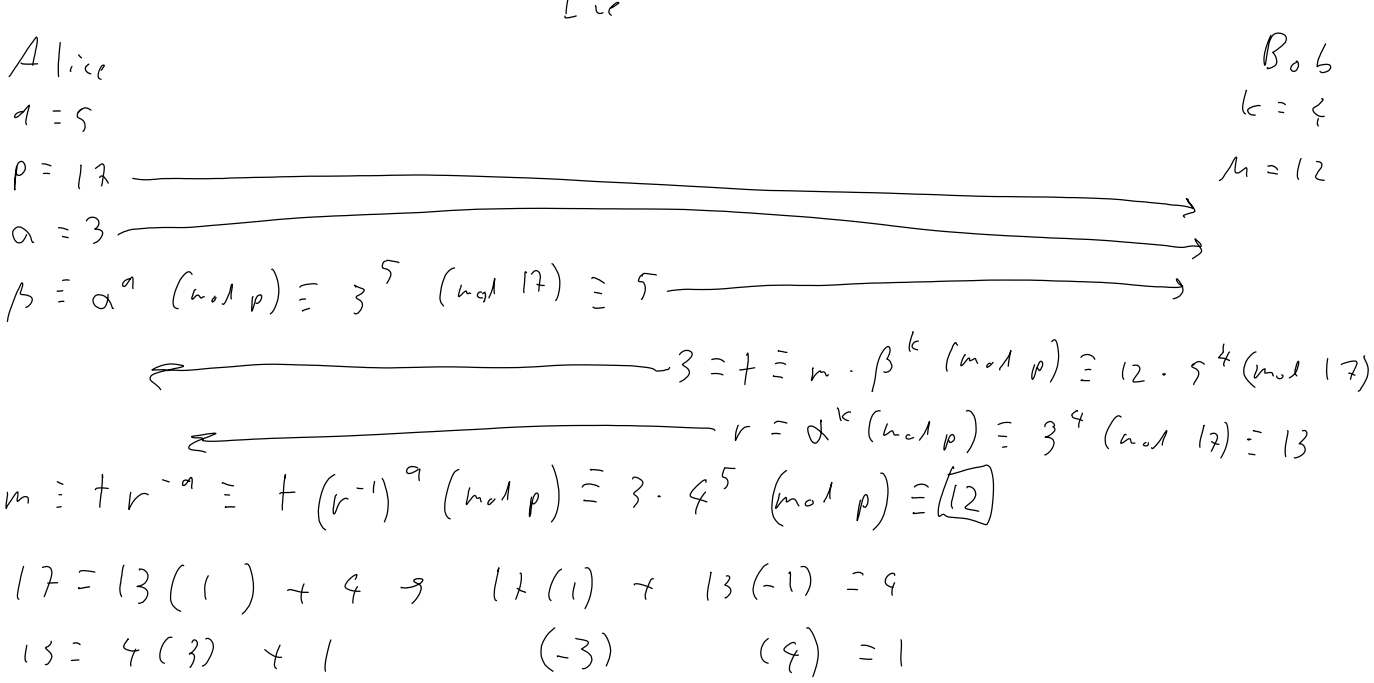
Example

Public Key: p = 17, α = 3, find β

Alice's secret: a = 5

Bob's secret: k = 4

M = 12



Practice

Public Key: p = 13, α = 4, find β

Alice's secret: a = 6

Bob's secret: k = 5

M = 12

Find β, t, r

Practice

Public Key: p = 23, α = 5, find β

Alice's secret: a = 7

You received t = 2 and r = 8 from Bob

Find β, M

$$\beta = \alpha^{a} \pmod{p} \equiv 5^{7} \pmod{23} \equiv 17$$

$$m = t \cdot r^{-a} \pmod{p} \equiv 2 \left(8^{-7}\right) \equiv 2 \cdot 3^{7} \equiv 4$$

a

k

α = generator

p = prime

$\beta = \alpha^{a} \pmod{p}$

$t = m \cdot \beta^{k} \pmod{p}$

$r = \alpha^{k} \pmod{p}$

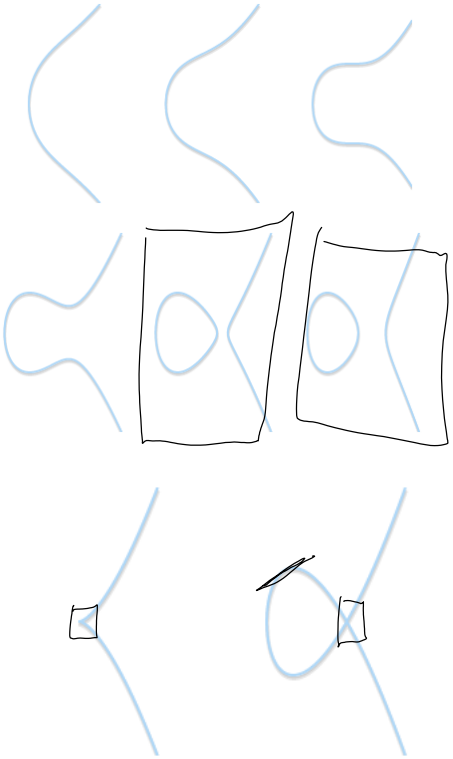
$m = t \cdot r^{-a} \pmod{p}$

Elliptic Curves

Wednesday, October 11, 2023 1:10 PM

Reminder PEX3 is due next week (don't start it at the last minute)

What is an elliptic curve? $y^2 = x^3 + ax + b$



$$\{(x,y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b,\ 4a^3 + 27b^2 \neq 0\} \cup \{0\}$$

Groups:

What is a group?

Addition must satisfy:

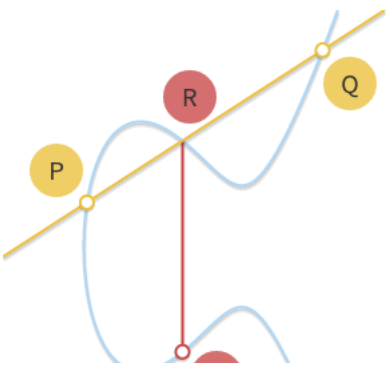
1. Closure
2. Associativity $(a+b)+c = a+(b+c)$
3. An existant identity element $a+0 = a$
4. An inverse $a+b=0$ $a+(-a)=0$

To get an Alebian Group add:

5. Commutativity $a+b = b+a$

Let's make an Alebian Group!

Set of points:
Identity Elements:
Inverse:
Addition:



$P + R + Q = 0$

$P + Q = -R$

$R = (x, y)$

$-R = (x, -y)$

-R

$O + Q = O$

$P + Q = -Q + Q = O$

What if P = 0?
What if P = -Q?
What if P = Q?

Now we can do math graphically.
Lets do it algebraicly!

$P + Q$

First we have to find the slope:

m = rise/run = $\frac{y_Q - y_P}{x_Q - x_P}$

Does this work if P = Q?

Let me save you time deriving these equasions:

$x_R = m^2 - x_P - x_Q$

$y_R = y_P + m(x_R - x_P) = y_Q + m(x_R - x_Q)$

Remember P + Q = -R NOT R

Lets check our formulas:

Our eliptic curve is $y^2 = x^3 - 7x + 10$
P = (3,4)
Q = (2,2)
What is P + Q?

$m = \frac{4 - 2}{3 - 2} = \frac{2}{1}$

$x_R = 2^2 - 3 - 2 = 4 - 5 = -1$

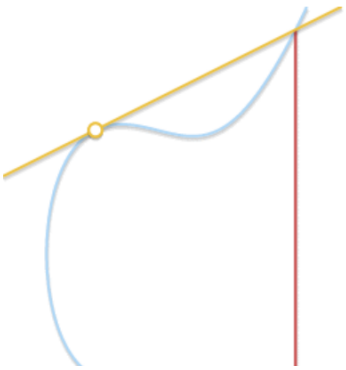
$y_R = 4 + 2(-1 - 3) = 4 + -8 = -4$

$R = (-1, -4)$

$-R = (-1, 4)$

You try. You the same Elliptic Curve: $y^2 = x^3 - 7x + 10$
P = (5,10)
Q = (1,2)
What is P+Q?

When P = Q, what is m?



$y^2 = x^3 + ax + b$

m = $\frac{3x_P^2 + a}{2y_P}$

Lets test this:

Our eliptic curve is $y^2 = x^3 - 7x + 10$

P = (-3,2)

Let's find P+P

$$m = \frac{3(-3)^2 + (-7)}{2 \cdot 2} = \frac{20}{4} = 5$$

$$x_R = 5^2 - (-3) - (-3) = 25 + 6 = 31$$

$$y_R = 2 + 5(31 - -3) = 172$$

$$-R = (31, -172)$$

$$P + P = 2P$$

Now you try:

Eliptic curve is $y^2 = x^3 - 7x + 10$

P = (3,4)

Let's find P+P

$$P + Q + R = 0$$

$$P + Q = -R$$

$$m = 2.5$$

$$x_R = .25$$

$$y_R = -2.875$$

$$-R = (.25, 2.875)$$

We can multiply now P+P = 2P

What is 11P?

$$1011_2 = 11_{10}$$

$$8P + 2P + P = 11P$$

$$2P + 2P = 4P$$

$$4P + 4P = 8P$$

11
8
3
2
1
0

What problem does this remind you of?

Is finding x where ~~nP = x~~ difficult for a computer?

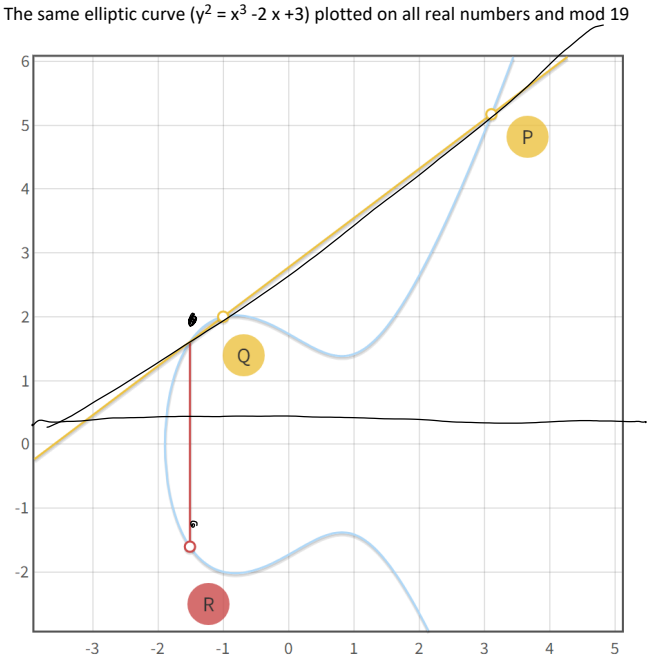
Is finding x where xP = Q difficult for a computer?

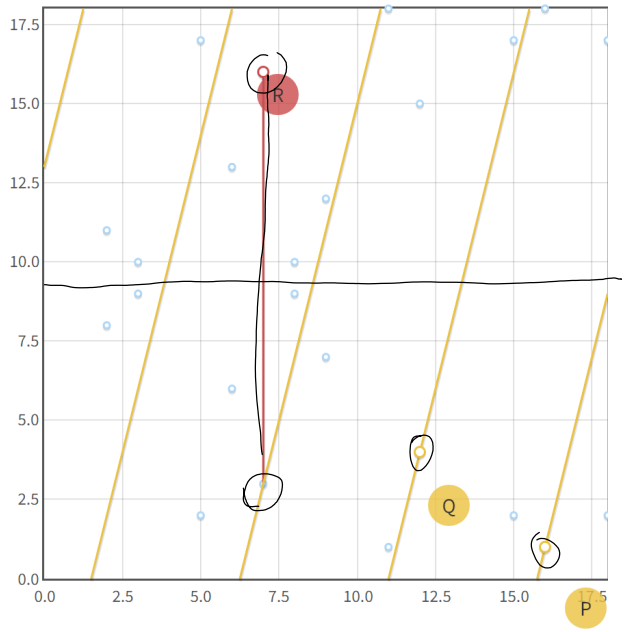
What kind of a function is this?

We call this a logarithm even though it is multiplication because of it's similarity to the log problem

We still have a problem.
Do you know mathmatical technique that allows us to operate using only integers?
Hint so far all of our cryptosystems have been using it.

The same elliptic curve ($y^2 = x^3 - 2x + 3$) plotted on all real numbers and mod 19

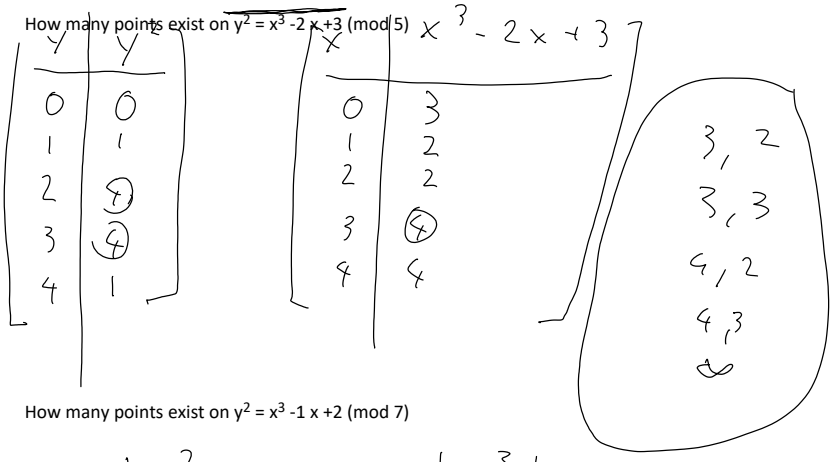




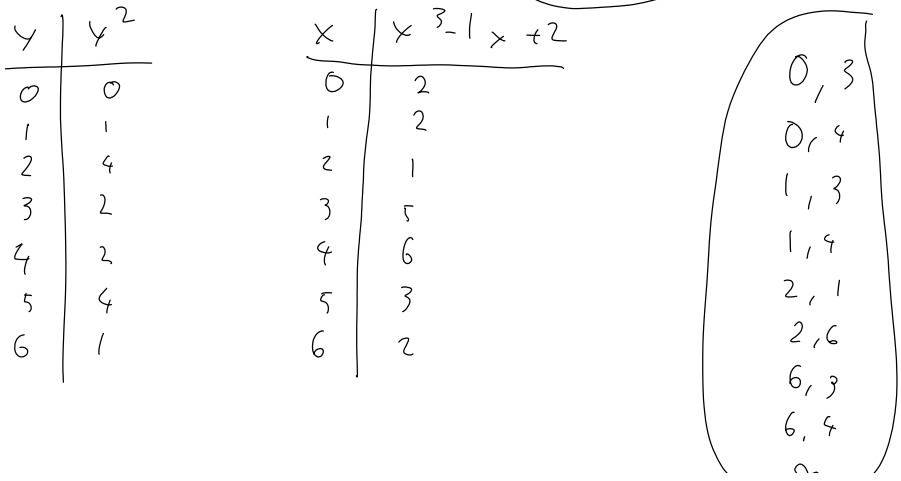
How many point are on the Elliptic Curve on the left?

There are 25 points on the Elliptic Curve on the right?

How many points exist on $y^2 = x^3 - 2x + 3 \pmod 5$



How many points exist on $y^2 = x^3 - 1x + 2 \pmod 7$



Lets see if our equations still work:
Our Elliptic Curve is: $y^2 = x^3 - 7x + 10 \pmod 7$
P = (5,3)
Q = (1,2)
What is P+Q?

$a = -7$

$b = 10$

$7 = 4(1) + 3 \rightarrow 7(1) + 4(-1)$

$4 = 3(1) + 1 \quad 7(-1) + 4(2)$

$$m = \frac{3-2}{5-1} = \frac{1}{4} = 4^{-1} = 2$$

$$x_R = 2^2 - 5 - 1 = -2 \equiv 5$$

$$y_R = 2 + 2(5-1) = 2 + 2(4) = 10 \equiv 3$$

$R = (5, 3)$

$-R = (5, -3) \equiv \boxed{(5, 4)}$

You try with the eliptic curve: $y^2 = x^3 - 7x + 10 \pmod 5$
P = (3,4)
Q = (2,2)
What is P + Q?

$$y_R = y_P + m(x_R - x_P)$$

$$y_R = y_Q + m(x_R - x_Q)$$

$m = 2$

$x_R = 4$

$y_R = 2 + 2(4-2) = 2 + 2(2) = 1$

$y_R = 4 + 2(4-3) = 4 + 2 \equiv 1$

$\boxed{-R = (4, 4)}$

Lets try multiplication:
Our eliptic curve: $y^2 = x^3 - 7x + 10 \pmod 7$
P = (6,4)
Find 5P

$P = (6, 4)$

$5P = 4P + P$

$4P = 2P + 2P$

$2P = P + P$

$$\frac{3(6)^2 - 7}{2(4)} = \frac{3}{1} = 3$$

$x_R = 3^2 - 6 - 6 \equiv 4$

$y_R = 4 + 3(4-6) = 4 - 6 \equiv 5$

$2P = (4, 2)$

$$\frac{3 \cdot 4^2 - 7}{4 \cdot 1 - 6} \quad 3$$

$\frac{}{2(2)} = \frac{}{4} = \frac{}{4} \equiv \frac{}{2} = 3(2) \equiv 3(-3) \equiv$

$7 = 2(3) + 1$

$X_R = 5^2 - 4 - 4 = 17 \equiv 3$

$Y_R = 2 + 5(3-4) \equiv 4$

$4P = (3, 3)$

$(3,3) + (6,4)$

$m = \frac{4-3}{6-3} = \frac{1}{3} = -2 = 5$

$7 = 3(2) + 1$

$X_R = 5^2 - 3 - 6 = 16 \equiv 2$

$Y_R = 3 + 5(2-3) \equiv 3 - 5 = 5$

$5P = (2, 2)$

You try:
Our eliptic curve: $y^2 = x^3 + 7x + 9 \pmod 5$
P = (2,1)
Find 2P

$(0, 3)$

Find 4P

$(4, 4)$

Find 6P

$(2, 4)$

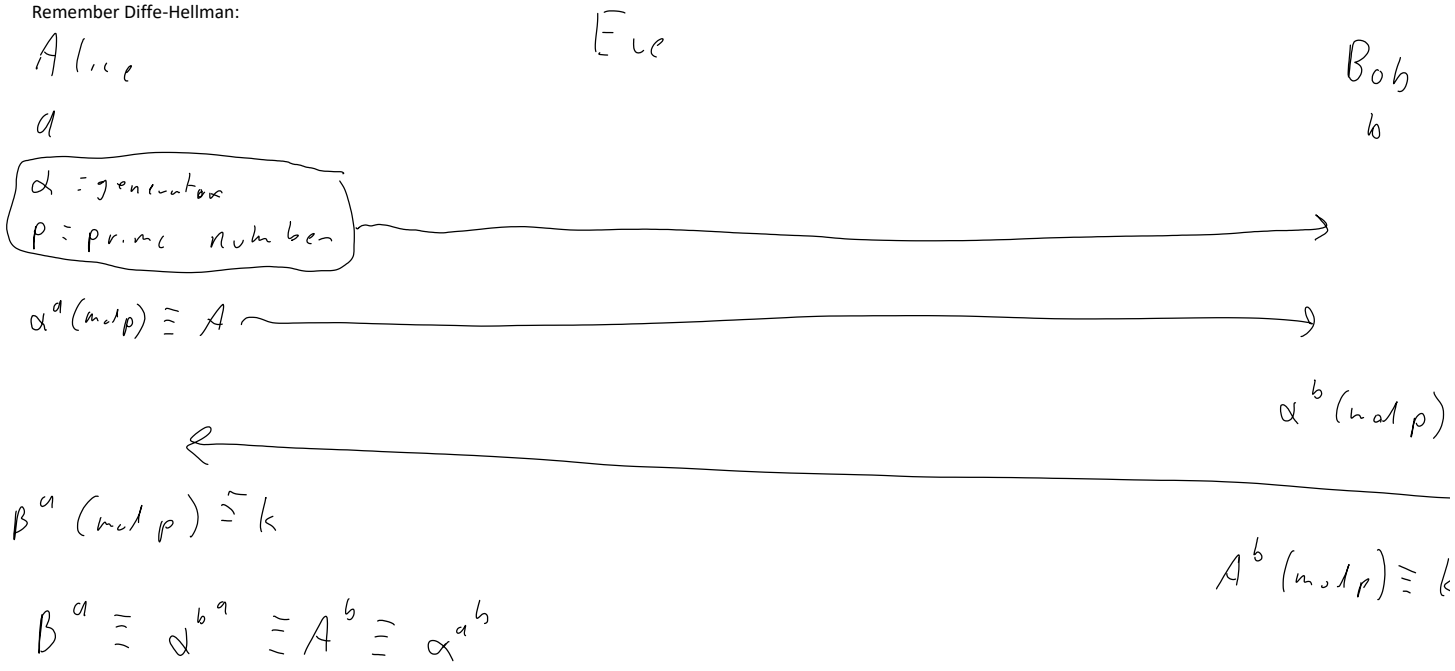
So everything still works!

Remember our Logerithm problem:

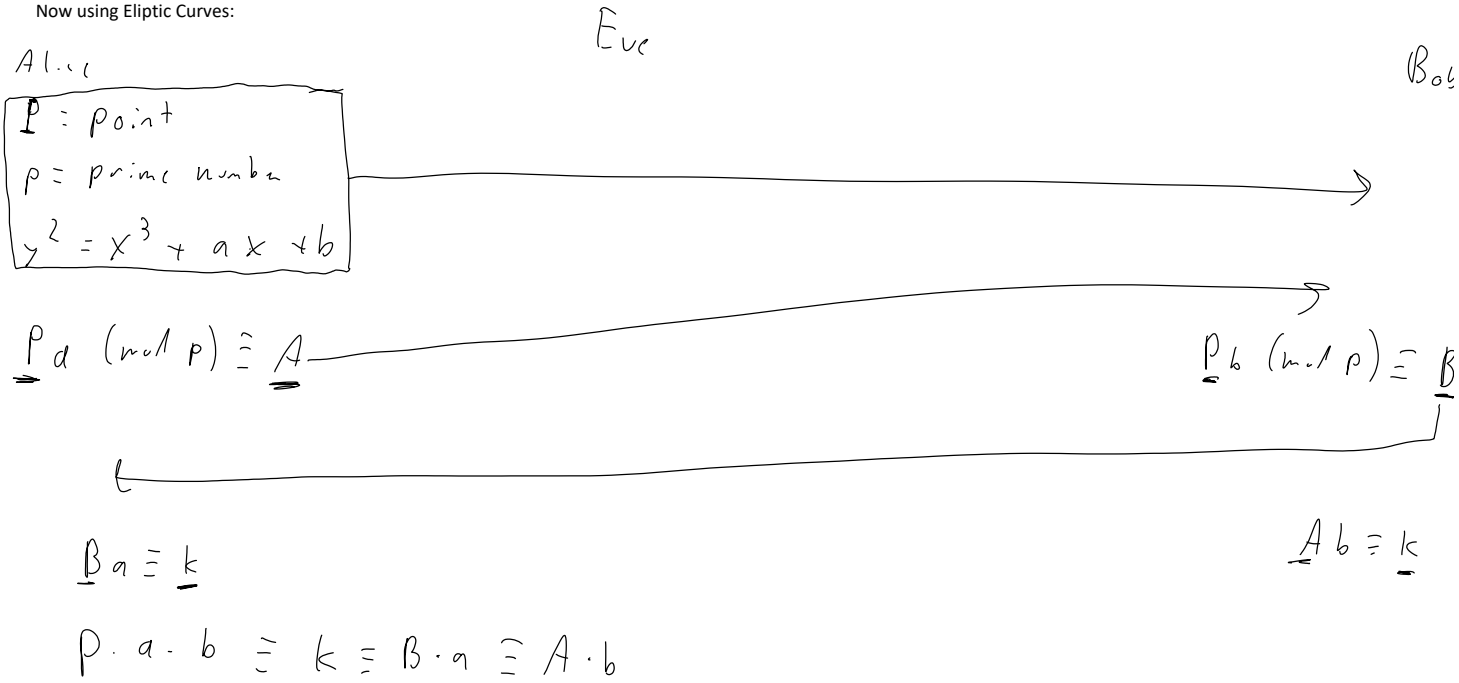
We are now using a field so our logerithm is now something else. What is it now?

This means we can implement Diffe-Hellman using Elliptic Curves!

Remember Diffe-Hellman:



Now using Eliptic Curves:



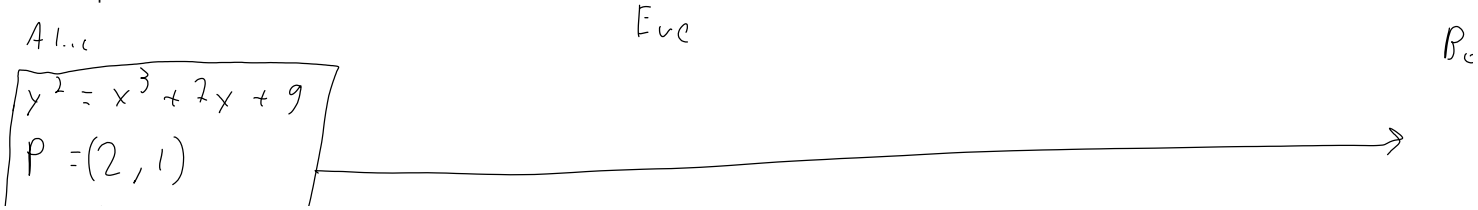
In this case what is the shared secret?

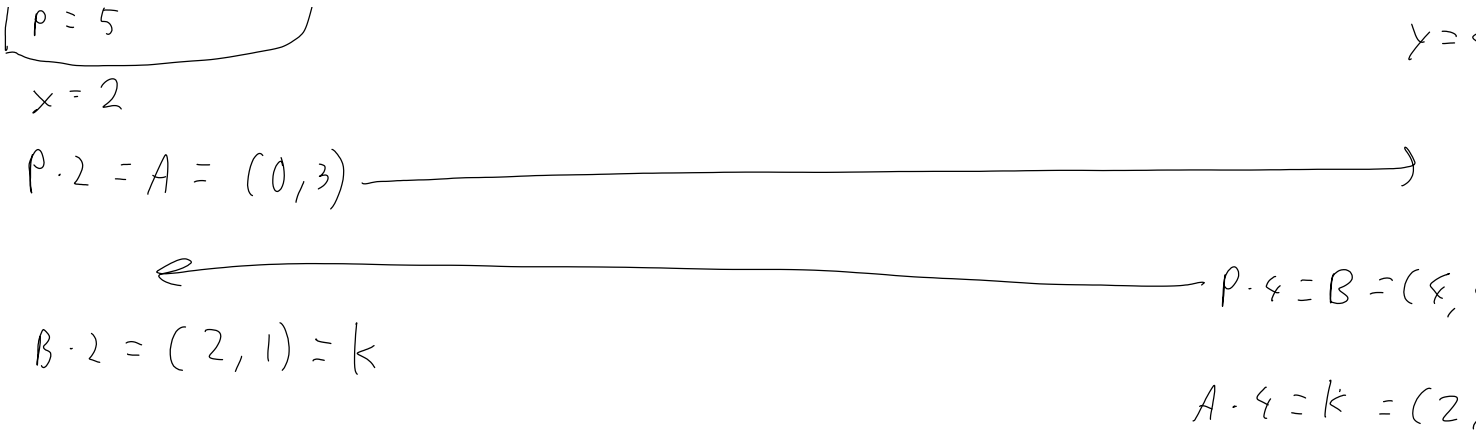
How is this useful?

I need to be careful with my choice for G because G creates a sub-group in my group

What happens if my subgroup is small?

Example:





You try:
Use: $y^2 = x^3 + 5x + 1$
p = 103
G = (36,22)

Do not tell your partner your secret, but see if you end up with the same shared secret.
Do not do the math by hand. Use: Elliptic Curve scalar multiplication ($\mathbb{F}_p$) (corbellini.name)
(The website that I used to design the lecture)

Why did we go through this very painful exercise of learning ECC?

Symmetric Key Size (bits)	RSA Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Recommended Key Sizes According to NIST

Baby Step Giant Step

Wednesday, October 18, 2023 3:08 PM

Reminder:
Homework is due on 3 November because of Exam 2
Make sure you are reading your books and working on the book report

Get in pairs
You try:
Use: $y^2 = x^3 + 5x + 1$
p = 89
P = (26,21)

Do not tell your partner your secret, but see if you end up with the same shared secret.
Do not do the math by hand. Use: Elliptic Curve scalar multiplication ($\mathbb{F}_p$) (corbellini.name)

Let say you want to break Diffe-Hellman, what problem do you need to solve?

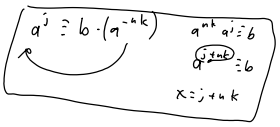
What about ElGamal?

What about Eliptic Curve Diffe-Hellman?

Lets look at a stratagy for solving this problem.
If we are given $\log_a(b) \equiv x \pmod p$, and need to find x.

1. Find N such that $n^2 > p-1$
2. Make a list of a^j for all integers j from 0 to n-1
3. Make a list of $b*a^{-nk} \pmod p$ for all integers k from 0 to n-1
4. Compare the list to see if you have a colision.
5. If you do: $x = j + n*k$

Why?



Example:
Solve $\log_4(5) \pmod{11}$

$\log_a(b) \equiv x \pmod p$

$a^x \equiv b \pmod p$

j	a^j
0	1
1	4
2	5
3	9

$b a^{-nk}$	k
5	0
9	1
	2
	3

$5 \cdot 3^{4 \cdot 1} \equiv 9$

$a = 4 \pmod{11}$
$b = 5$
$p = 11$

$n^2 > p-1 = 11-1 = 10$

$x = 2 + 4 \cdot 0 = 2$
$? \; 4^2 \equiv 5 \pmod{11}$
$x = 3 + 4 \cdot 1 = 7$
$? \; 4^7 \equiv 5 \pmod{11}$

$b \cdot a^{-nk}$
$5 \cdot 4^{-4k} \equiv 5 \cdot (4^{-1})^{4k}$

$11 = 4(2) + 3 \rightarrow 11(1) + 4(-2) = 3$
$4 = 3(1) + 1 \quad\quad 11(-1) + 4(3) = 1$

(2)

For my example how many calulations would a brute force require?

10

For mod 137 how many calulations would be required for a brute force?

$137 - 1 = 136$

How many calculations would BSGS require?

$12^2 = 144 > 137$

So why use BSGS?

You try:
Solve $\log_3(4) \pmod{11}$

$n = 5$

j	3^j
0	1
1	3
2	9
3	5

k	$4 \cdot 3^{-4k} = 4(3^{-1})^{4k} = 4 \cdot 9^{4k}$
0	$4 = 4$
1	$1 = 4^5$
2	$3 = 4^9$
3	$= 4^{13}$

$x = 9$?

$0 + 4 \cdot 1 = 4$

$1 + 4 \cdot 2 = 5$

$3^4 \equiv 4 \pmod{11}$

$3^9 = 4$

How could we apply this to Eliptic Curve Crypto?

What is our ECC Discrete Log Problem?

1. Find N such that $n^2 > p-1$
2. Make a list of jP for all integers j from 0 to n-1
3. Make a list of Q - knP (mod p) for all integers k from 0 to n-1
4. Compare the list to see if you have a colision.
5. If you do: x = j + N*k

$jP \leftarrow b^j$

$Q - k_n P \leftarrow a \cdot b^{-nk}$

Why?

$a^x \equiv b \pmod{p}$ find x

$xP = Q$ find x

$jP = Q - k_n P$

$jP + k_n P = Q$

$(j + kn)P = Q$ $\quad x = j + kn$

Lets test it!
Use: $y^2 = x^3 + 5x + 1$
p = 89
P = (26,21)

$y^2 = x^3 + ax + b$ $\quad n^2 > p - 1$

$xP = Q$ $\quad Q = (37, 51)$

j	jP
0	∞
1	(26, 21)
2	(47, 75)
3	
⋮	
10	

k	$-nkP$	$Q - nkP$
0	∞	
1	(0, 1)	(47, 75)
2		
⋮		
10		

$x = j + kn = 2 + 1 \cdot 10 = 12$

$(26, 21) = P$ $\quad 2P = P + P$

(1) $m = \frac{3x^2 + a}{2y} = \frac{3 \cdot 26^2 + 5}{2 \cdot 21} = \frac{2033}{42} \equiv 59$

$89 = 42(48) + 17$ $\quad 42^{-1} \equiv -36 \equiv 53$

(2) $x_R = m^2 - x_P - x_Q = 59^2 - 26 - 26 \equiv 47$

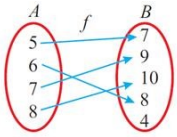
$y_R = 21 + 59(47 - 26) \equiv 14$

(3) $-R = (47, 75)$

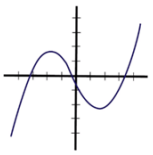
Hashes

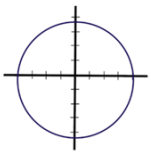
Monday, October 23, 2023 9:16 AM

What is a function?



Is this a function? Is this a function?





Function maps X -> Y

Domain -> Codomain/Range

Are functions always "one-to-one"?

For a hash function: range is much smaller than the domain

What does this mean? $H(m_1) = H(m_2)$

1. Collisions (Not One-to-One)
2. Shrinks more information to less
3. It's a true one function (vs. a trap door function)

Example:

Pick a random 3 digit number

Take that number mod 5

Properties of a good hash function:

1. Quick - Why is this important?
2. One way, given a y it should be infeasible to find an m' with h(m') = y
3. Collision Free
   a. Strongly Collision Free, hard to find m1 and m2 with h(m1) = h(m2)
   b. Weakly collision free – given x, hard to find x' ≠x with H(x') = h(x)

Why are hashes useful?

1. Document verfification
2. Password storage
   a. Why not store passwords in plaintext?
   b. Why not encrypt passwords?

Hashing passwords is not perfect:

1. What is two users have the same password?
2. What is someone precomputes hashes?

Salting a hashtable

Hash overview

Hash	Created	Author	Output size (bits)
MD4	1990	Rivest (R from RSA)	128
MD5	1992	Rivest	128
SHA1	1995	NSA	160
SHA2	2001	NSA	224,256,384,512
SHA3	2016	Bertoni, Daemen, Peeters, and Van Assche	Variable

Windows Hashes:

The LM hash process:

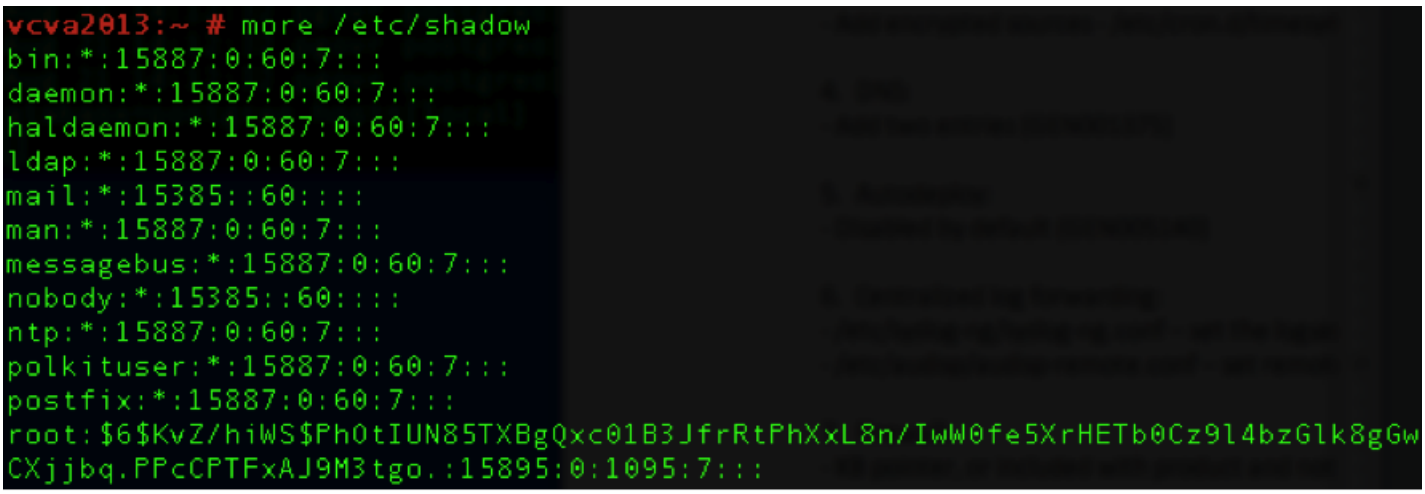
1. The user's password is restricted to a maximum of fourteen characters.
2. The user's password is converted to uppercase.
3. This password is NULL-padded to 14 bytes.
4. The "fixed-length" password is split into two 7-byte halves.

5. These values are used to create two DES keys, one from each 7-byte half, by converting the seven bytes into a bit stream with the most significant bit first, and inserting a parity bit after every seven bits. This generates the 64 bits needed for a DES key.
6. Each of the two keys is used to DES-encrypt the constant ASCII string “KGS!@#$%”.
7. These two ciphertext values are concatenated to form a 16-byte value, which is the LM hash.

The NTLM hash is a MD4 hash of the little endian UTF16 encoded password

Linux Hashes:

/etc/passwd or /etc/shadow



Root:6KvZ/hiWS$Ph0tIUN85TXBgQxc01B3JfrRtPhXxL8n/IwW0fe5XrHETb@Cz914bzGlk8gGw9CXjjbq.PPcCPTFxAJ9M3tgo:158...

User

Hash type

1 is Message Digest 5 (MD5)
$2a$ is blowfish
5 is SHA-256
6 is SHA-512
y or 7 is yescrypt
none means DES

Salt

Hash

ECDH Break using BSGS (rough notes)

Wednesday, October 25, 2023 2:22 PM

ECDH Ecc

Alice

$y^2 = x^3 + 5x + 7 \pmod{19}$

$P = (3, 7)$

$x = 15$

$A = 15(3,7) = (2,14)$

$xP = A$

Bo

y:

(0, 8) : yP :

$B_x = k = (0,8)\,15 = (12,3)$

$A_y = k = xP_y = xyP = B_x = yPx = xyP$

Ay :

(2,14) 2 = (12

$15P$

$P + P = 2P$

$2P + 2P = 4P$

$4P + 4P = 8P$

$8P + 4P = 12P$

$12P + 2P = 14P$

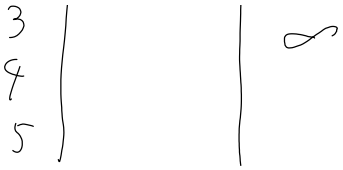
$14P + P = 15P$

$p - 1 < n^2$

$xP = A$

j	jP
0	∞
1	(3, 7)
(2)	(0, 8)

k	-nkP	A - nkP
0	∞	(2, 14)
(1)		(0, 8)
2		



Digital Signatures

Monday, October 23, 2023 9:16 AM

Announcements:

Exam 2 still being graded

For next lecture please:

1. Install hashcat (https://hashcat.net/hashcat/)
2. Download rockyou.txt from d2l

Reminder: PEX4 due Nov 15th

Reminder: Paper due Dec 4th (Please come to the writing center for help on Nov 2nd, Nov 8th, Nov 27th)

What technologies have been used throughout history for signatures?

Why can't we simply digitize our signature and attach it to a file?

We need a signature attached to a very specific document.

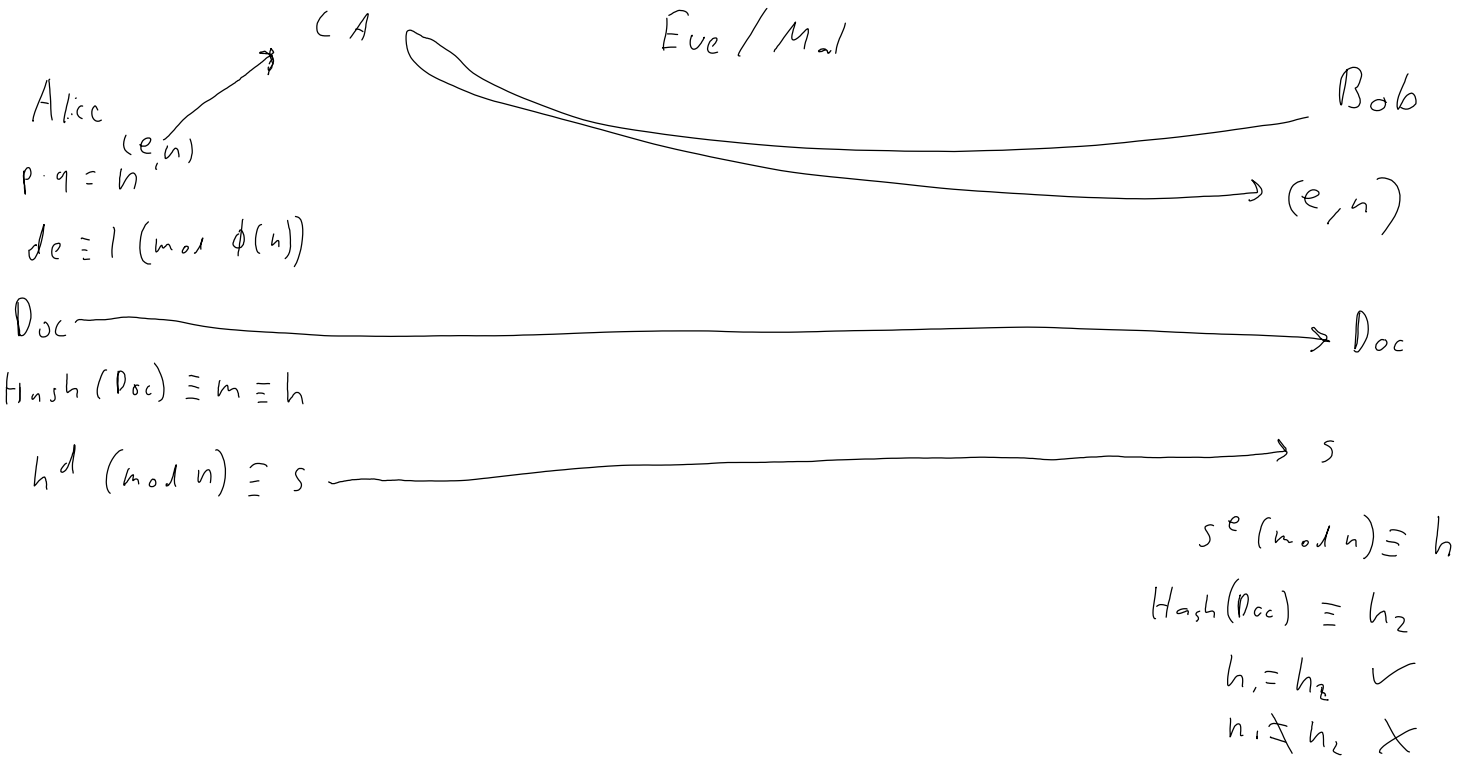
Do we have a way of "fingerprinting" a document to make sure it has not been edited?

Digital signing involves two distinct processes:

1. signing process
2. verification process.

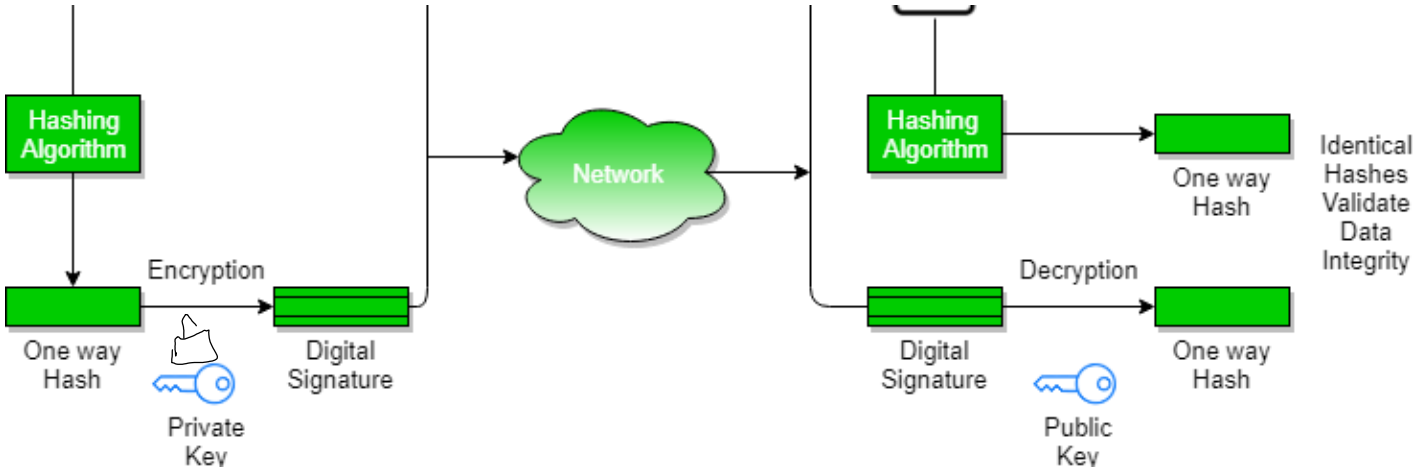
Let's do a demo!

RSA signature:



Can ElGamal also be used?

Recap:


Hashing Algorithm
Network
Hashing Algorithm
One way Hash
Identical Hashes Validate Data Integrity
Encryption
Decryption
One way Hash
Digital Signature
Digital Signature
One way Hash
Private Key
Public Key

Breaking Hashes

Wednesday, November 01, 2023 9:19 AM

Hashes are used for at least 2 purposes:

1. Doc verification
2. password storage

Let's talk about #1 first:

(Pay attention: you will need this for PEX4)

Document #1 -> Hash Function -> Hash #1

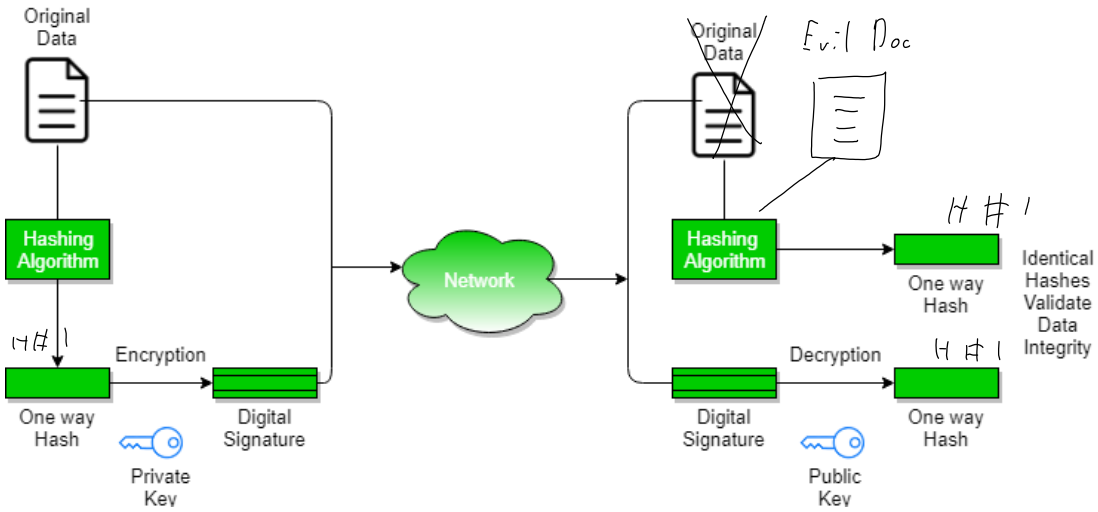
Document #2 -> Hash Function -> Hash # 2

Breaking a hash in this scenario means:

Document #1 -> Hash Function -> Hash #1

Document #2 -> Hash Function -> Hash # 1

Remember:



Birthday attack

Uses the birthday paradox

Probability of two people having the same birthday:

$$1 - \left(\frac{365}{365} \cdot \frac{364}{365}\right) = .0027$$

Probability of two people having the same birthday in a group of three:

$$1 - \left(\frac{365}{365} \cdot \frac{364}{365} \cdot \frac{363}{365}\right) = .0082$$

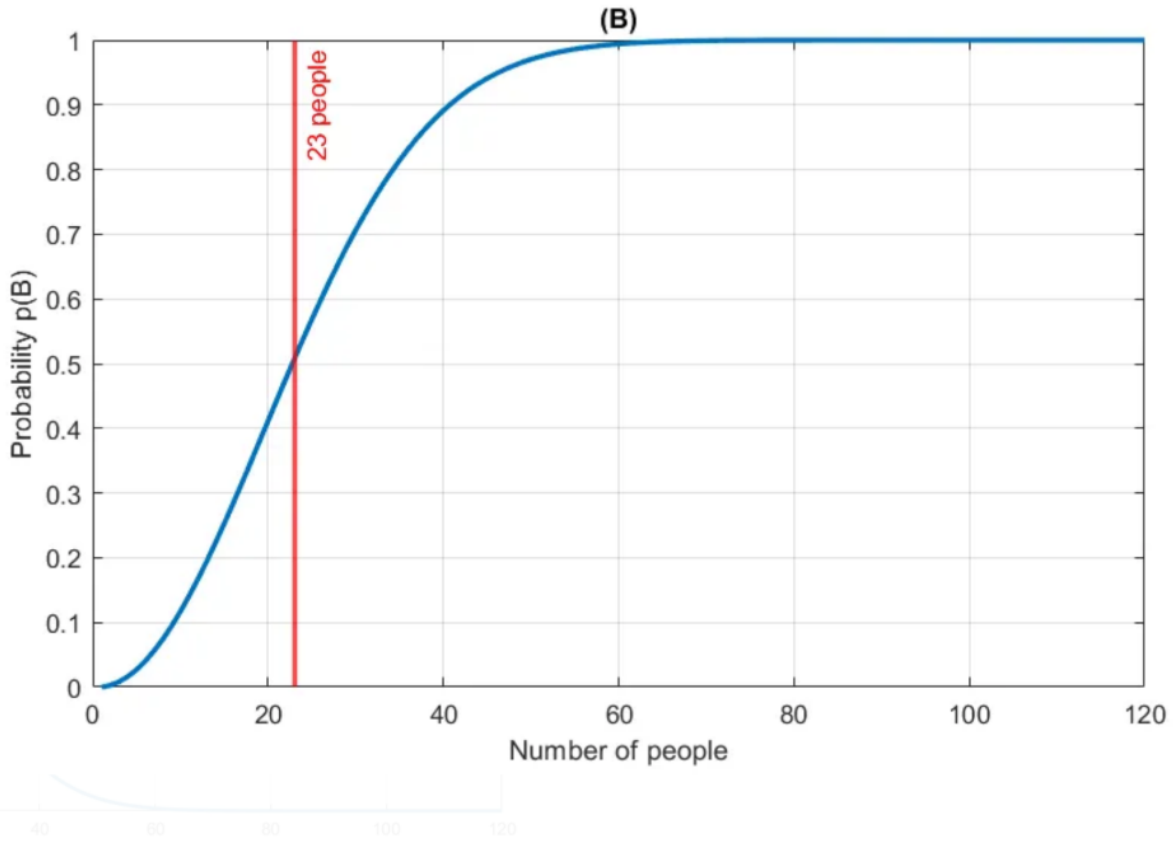
Probability of two people having the same birthday in a group of four:

Probability of two people having the same birthday in a group of n:

$$1 - \left(\frac{365!}{365^n \ (365-n)!}\right)$$

Probability of two documents having the same hash:

$$1 - \left(\frac{x!}{x^n (x-n)!} \right)$$



PEX4 will have you do this with the last 20 bits of the hash

We know how to break document signatures.
What else are hashes used for?

Any ideas how to crack these hashes?

We will learn 4 techniques (but more exist):

1. Dictionary attack
2. Brute force
3. Pass the Hash
4. Rainbow Table

Hashcat (Techniques 1 & 2):

89904b465c7eaac850a66573969d8bcb:sleepless

aca774b61bdeaacebcd784b4924e337d:Sleepless

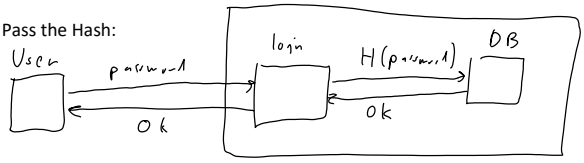
64aa58be3cb1b70531bdd57e8d24e31c:Sleepless2

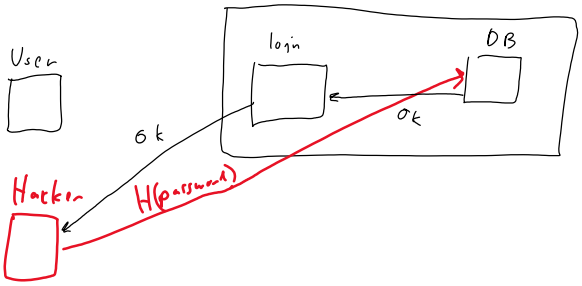
15c6f8ebe16291e80c4e6115053e8992:sle2@

cd36cb02bb2eaf77bbbc7a73c5e44087:sleeplessleepless

c98202ae9144c26940614c9389e9e32d02f61652:sleepless1

Pass the Hash:

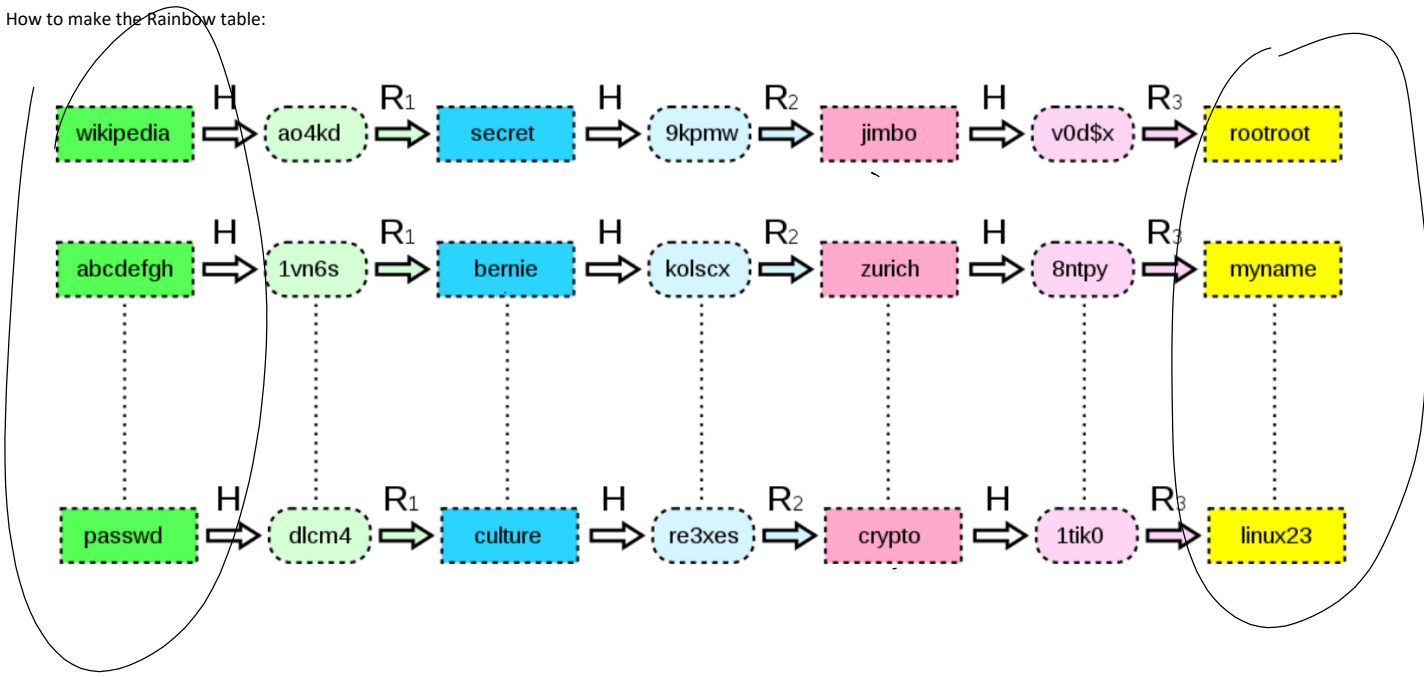




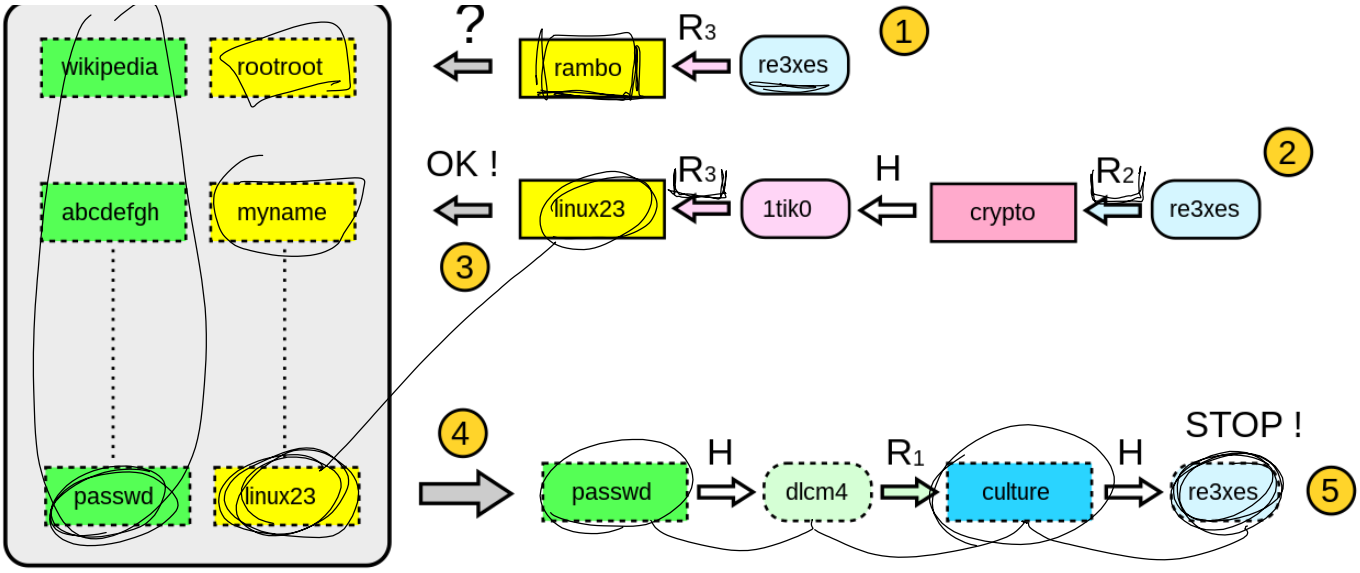
Rainbow tables:

2 steps

How to make the Rainbow table:



How to check a hash:



Why are Rainbow Tables more efficient than just saving hashes in a table?

Tools

Thursday, November 2, 2023 11:15 AM

Announcements:

Make sure you have openssl working on your laptop

Hashcat:

89904b465c7eaac850a66573969d8bcb

aca774b61bdeaacebcd784b4924e337d

64aa58be3cb1b70531bdd57e8d24e31c

15c6f8ebe16291e80c4e6115053e8992

cd36cb02bb2eaf77bbbc7a73c5e44087

c98202ae9144c26940614c9389e9e32d02f61652

You try:

This user used a common password. Here is his MD5 hash:

a86842258f5ee32f78b864bc0ac488b0

This user also used a common password but used a SHA1 hash:

7fc80bc56596d3cff5176245577520d54c96db5e

This user used c ommon password but appended 3 digits to the end to make it impossible to guess. Here is his MD5 hash:

c7d974a5a786e2898275229a3f2a8586

This user is a huge fan of the Song of Roland. His password is the names of his two favorite Paladins appended together. Here is his MD5 hash:

fcb71c38c722ed41a04019236f407570

Here are a list of Charlemagne's Paladins:

Roland
Oliver
Gerin
Gerier
Grandonie
Berengier
Otton
Samson
Engelier
Ivon
Ivoire
Anseis
Girard
Turpin
Ogier

Good luck guessing this users password. All I know it's a 4 letter string with the first letter capitalized followed by a number then a symbol. Here is his MD5 hash:

1f20656dc8b85feb63c211f100442b22

Let's go over MATLAB and Python commands. I will give some examples of RSA encryption.

Python

Modular Exponentation

pow(a,b,n)

Modular Multiplicative Inverses

pow(a,-1,n)

Converting decimal to hex and back

Int("",16)

Hex()

Converting decimal numbers to strings and back

```
decimal_num = int("".join([hex(ord(i)).strip("0x") for i in text]),16)

text = "".join([chr(int(hex(decimal_num).strip("0x")[2*i:2*i+2],16)) for i in
range(int(len(hex(decimal_num).strip("0x"))/2))])
```

Matlab (not recommended)

Modular Exponentation

powermod(a,b,n)

Modular Multiplicative Inverses

powermod(a,-1,n)

Converting decimal to hex and back

hex2dec()

dec2hex()

Converting decimal numbers to strings and back

```
decimal_num = hex2dec(reshape(dec2hex(text).',1,[]))

text = reshape(char(hex2dec(reshape(dec2hex(decimal_num),2,[]).')),1,[])
```

I will always give message in ASCII and everything else in hex.

Here is an example:
Use an RSA key with p = 0x2FAFD25, q = 0x467F4F5, and e = 0x10001 to encrypt m = "Coast Guard".

Now decrypt the following RSA encrypted ciphertext:

C = 0x2c38c490988a

The public key is (E = 0x10001, N = 0x2de24fbb6983)

Hint: I used twin primes

OpenSSL

Monday, November 6, 2023 9:38 AM

Anouncement:

3 more tools!

1. GPG
2. pgpdump
3. Aircrack-ng suite

Homework 9 has been graded

What is RSAs private key?

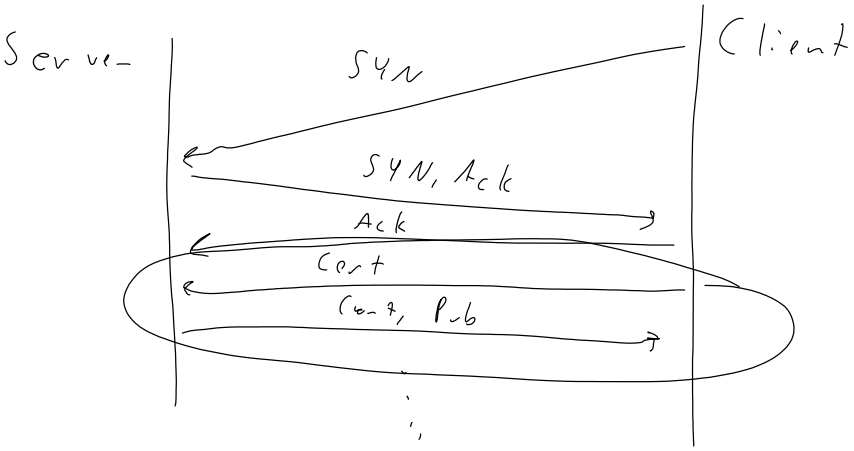
Goal with OpenSSL -> Generate keys (correctly and incorrectly) and certificates

What is HTTP?

What is HTTPS?

What is used to encrypt HTTPS?

How does TLS work?



The server needs a private key to sign and encrypt. OpenSSL is often how the key pairs are generated.

Why OpenSSL covered in this class?

1. This is where the mathmatical theory intersects with practice
2. If you become a cyber officer you will deal with OpenSSL certificates

A OpenSSL ~~key~~ file looks like this:

_badssl - Notepad

File Edit Format View Help

```
-----BEGIN CERTIFICATE-----
MIIE8DCCA9igAwIBAgISA4mqZntfCH8MYyIVqUF1XZgpMA0GCSqGSIb3DQEBCwUA
MDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQD
EwJSMzAeFw0yMzEwMTkxNTUwMjlaFw0yNDAxMTcxNTUwMjhaMBcxFTATBgNVBAMM
DCouYmFkc3NsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAONj
dsqxZsR+pDzWX6GLCy6ImoAT60LNYvs9U6BIQ+fatIWbMELAFD6jY+IP25hrVEr1
bgwRWmAAOnUc2qKXdtx6KXXO3cAJoCSHFNBDEZqzg/+exj+3emQH8dVZiYAS2Rpd
nL9uKc3xgDDb74p1m7J4JdMewHmebRUmMt0MbA0f8sxvhbv9wIXkgAZd6dKYPGzJ
KJlCoQifPiJ66JwYk8WVGEJH9m8LNDse388MscfsuwvAAh9tt2Fq6rmV9s21P6qf
JgjePl65e8fVjsEWBAvC/aMYvTUs7Gdqej0qByjESpt1LZClNomJDvIgqA9+5KsU
yCXigT6OiPjtZhdhgw0CAwEAAaOCAhkwggIVMA4GA1UdDwEB/wQEAwIFoDAdBgNV
HSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADAdBgNVHQ4E
FgQUqryJ2HM8bXniU+mPXLakkgUQobMwHwYDVR0jBBgwFoAUFC6zF7dYVsuuUAlA
5h+vnYsUwsYwVQYIKwYBBQUHAQEESTBHMCEGCCsGAQUFBzABhhVodHRwOi8vcjMu
by5sZW5jci5vcmcwIgYIKwYBBQUHMAKGFmh0dHA6Ly9yMy5pLmxlbmNyLm9yZy8w
IwYDVR0RBBwwGoIMKi5iYWRzc2wuY29tggpiYWRzc2wuY29tMBMGA1UdIAQMMAow
CAYGZ4EMAQIBMIIBAwYKKwYBBAHWeQIEAgSB9ASB8QDvAHUA2ra/az+1tiKfm8K7
XGvocJFxbLtRhIU0vaQ9MEjX+6sAAAGLSNh8nwAABAMARjBEAiBkJnQowOqs+tDj
7qXXu0PlDCvgvtEemuw1OvInlaHSrAIgcCZV5dJmGVrS1voinEpAzScJejhGB0vb
G8dfKhJZD+wAdgA7U3d1Pi25gE6LMFsG/kA7Z9hPw/THvQANLXJv4frUFwAAAYtI
2HyZAAAEAwBHMEUCIQCJ+gamX0P/hGiIuu70hn8d0svHSOAMJs3D+eOjMVqsywIg
JXR/lAknUTRU+SyfySDoQ22bDSXfYWZGHLFgAkiRo48wDQYJKoZIhvcNAQELBQAD
ggEBAGE3PDg7p2N8aZyAyO0pGVb/ob9opu12g+diNIdRSjsKIE+TO3uClM2OxT0t
5GBz6Owbe010MQtqBKmX4Zm2LSLUm1kVhPh2ohWmA4hTyN3RG5W0IJ3red6VjrJY
URhZQoXQb0gonxMs+zC+4GQ7+yqzWA1UkrWrURjjJCuljyoWF9sE7qEweomSQWnV
v6bIF599/di1R2l5vcRq1DsQDgKaFY4IpKnvh3RhgO19YxlSS9ERRGBem3Aml9tb
Yac12RmyuxsEAr0v75YeL3pAuq/1Rd5OeKfkm+K06Px3LxwcF92RljXkH6T2U8VM
PEFKedHjYjAag3DUMqSuuGI+ONU=
```

```
-----END CERTIFICATE-----
```

Ln 13, Col 49 | 100% | Windows (CRLF) | UTF-8

Is this a certificate, a public key or a private key?

Distinguished Encoding Rules (DER) vs. Privacy Enhanced Mail (PEM)

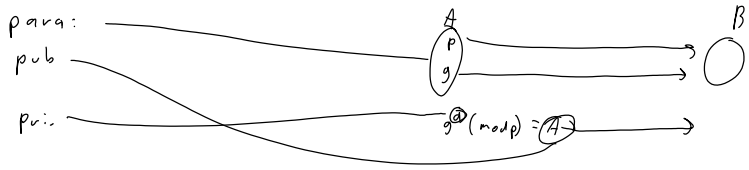
How to generate keys and certs:

First run: $ openssl

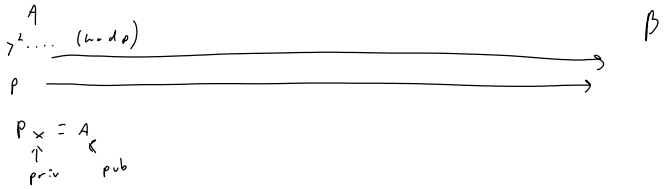
What do you see? What do you recognize?

Generate an RSA key with genrsa, insepct with rsa

Generate a DH key with dhparam and genpkey, inspect with pkey



Generate a ECDH key with ecparam, inspect with ec



What asymetric cryptosystem did we not use?

This cipher is relatively secure. How would we generate a custom private key?

Use asn1parse and the file I uploaded on d2l

Note:

e1= d mod (p-1)

e2= d mod (q-1)

coeff = q^(-1) mod p

We have a bunch of private keys. Why do we have to generate private keys before generating public keys?

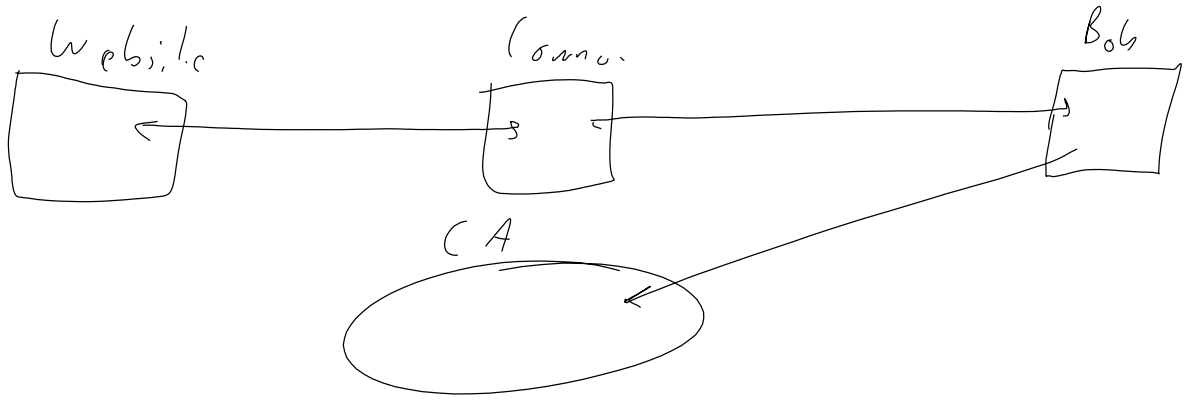
Let generate some public keys:

Use rsa for RSA

Use pkey for DH

Use ec for ECDH

Typically you need your public key to be signed by a Certificate Authroity.



Why is this important practically?

Why is it improtant from a security perspective?

Let take a look at a website: badssl.com

Let's create our own certificate. Why is this not a good idea in practice?

Use req -new to create a certificate signing request (CSR)

Use x509 -req to create the certificate

How would you use these certificates?

GPG

Wednesday, November 8, 2023 1:25 PM

OpenSSL generates keys and certificates for what?

In practice encrypted files and signed files are signed using PGP.

GNU Privacy Guard (GPG) is an implementation of OpenPGP

Lets use GPG to generate a PGP key:

```
gpg  --full-generate-key
```

This generates both a private and public key.

View keys private/public with -K/-k

GPG uses the word "secret" instead of private keys. Why?

Key can be used to signed with different options:

1. cleartext (--clearsign) vs. encoded
2. detached (-b) vs. attached

An encoded, attached signature is specified with -s

What is the difference between encryption and encoding?

Signatures can be verified using the --verify flag or the -d flag.

GPG does 2 types of encrypting: symetric (-c) vs. asymetric (-e)

Decryption occurs with a -d flag.

Encryption and signatures can be combined.

Keys can be exported using --export for public keys and --export-secret-keys for private keys

Keys can be imported with --import

CG Crypto Tools

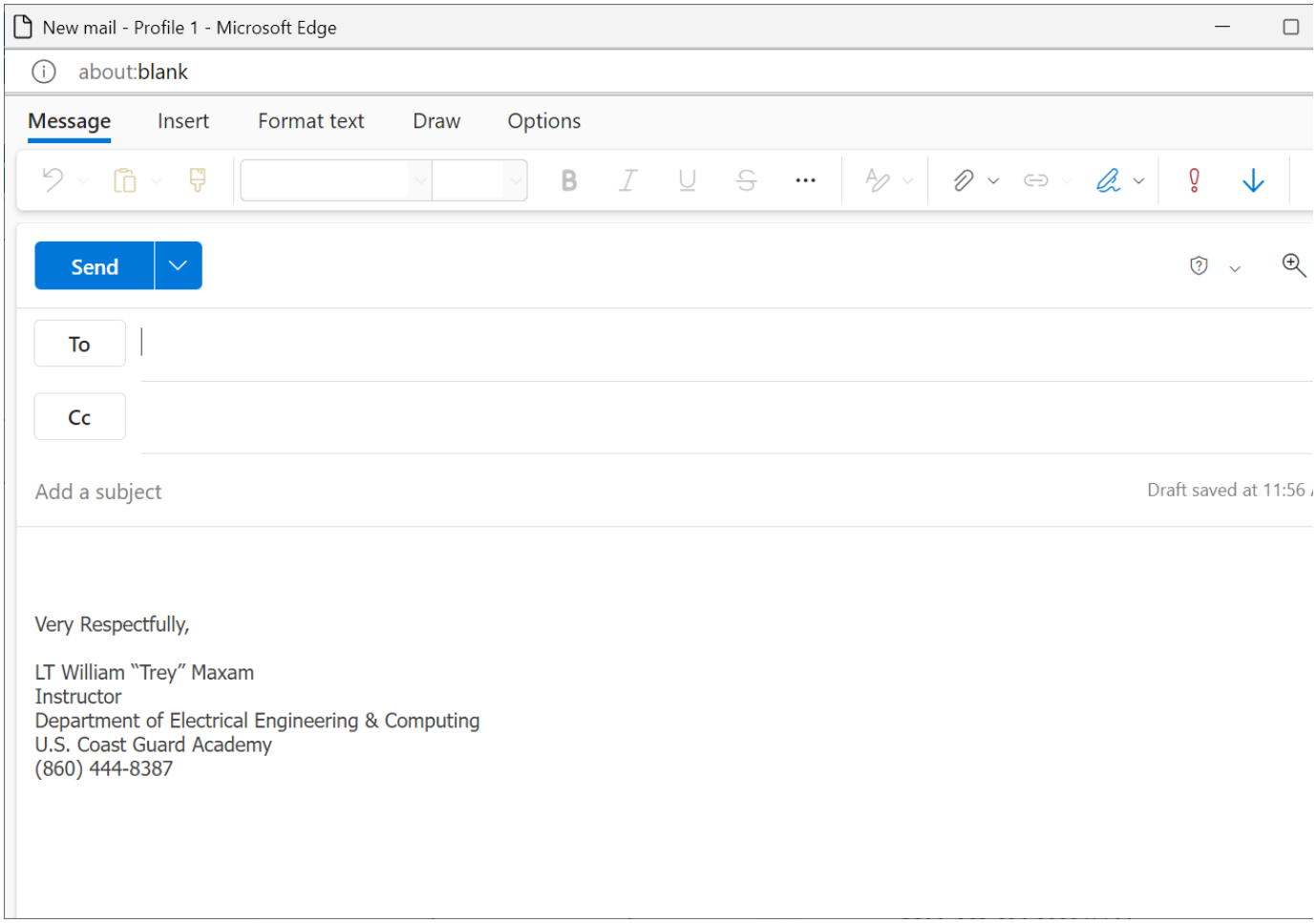
Wednesday, November 15, 2023 11:51 AM

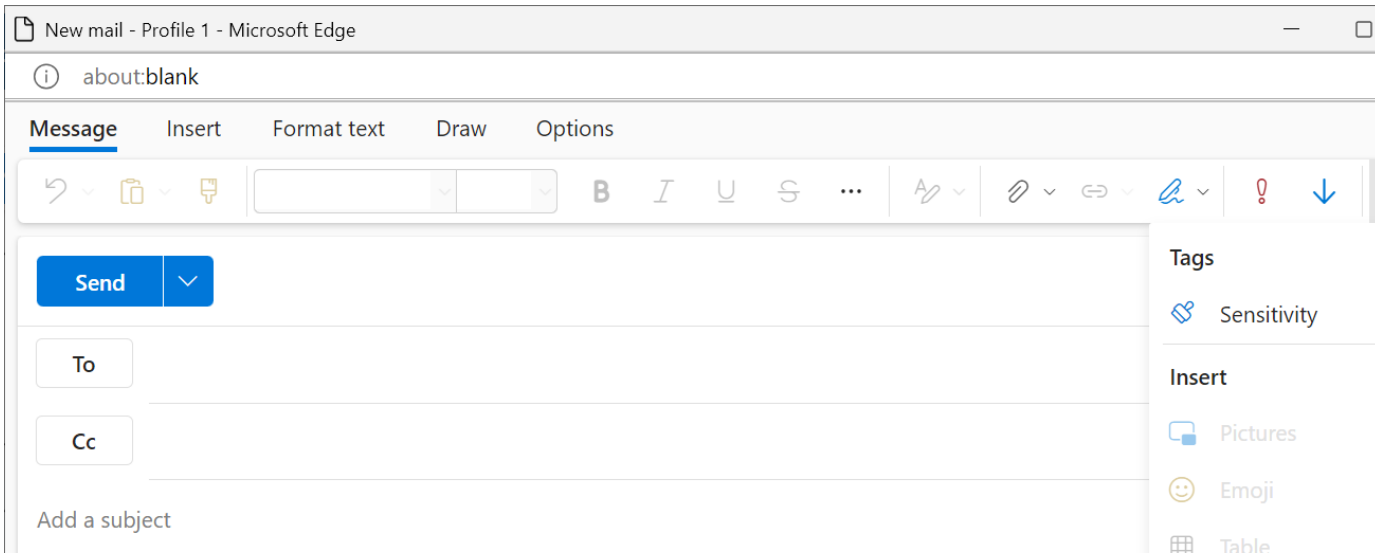
4 tools often used for signing and encrypting.

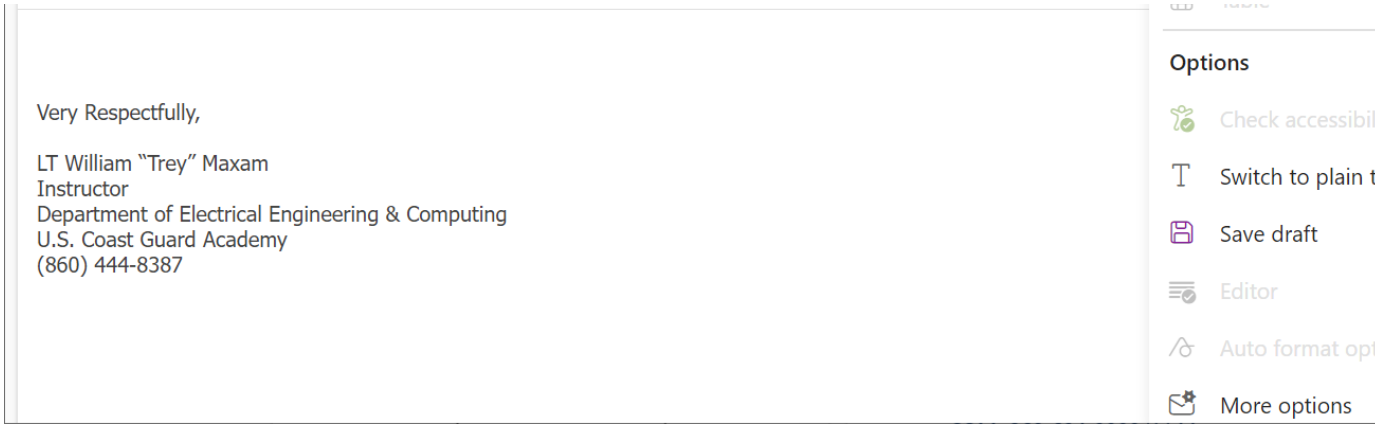
Why sign and encrypt in the CG?

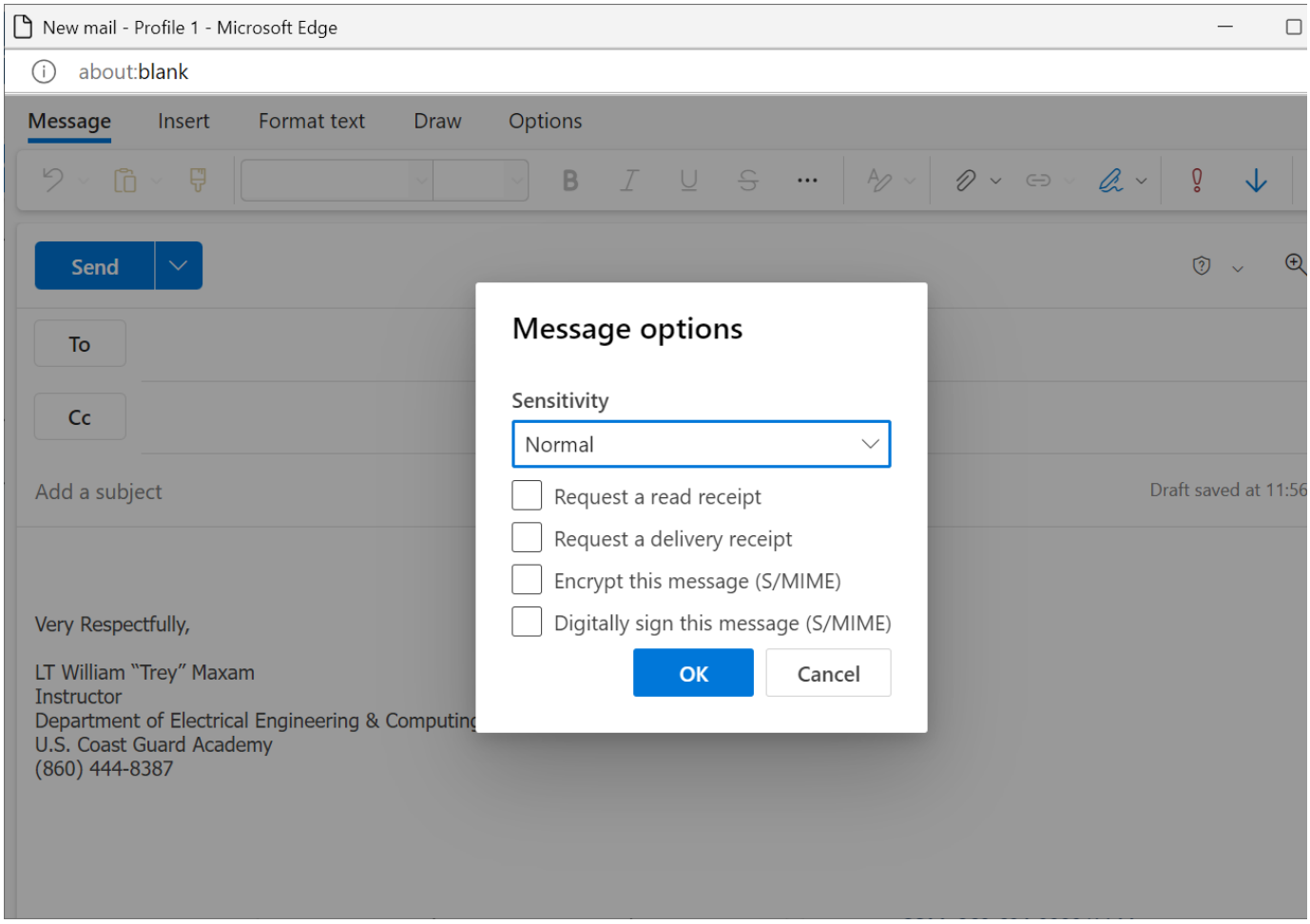
Outlook

- What does signed/encrypted mail look like?







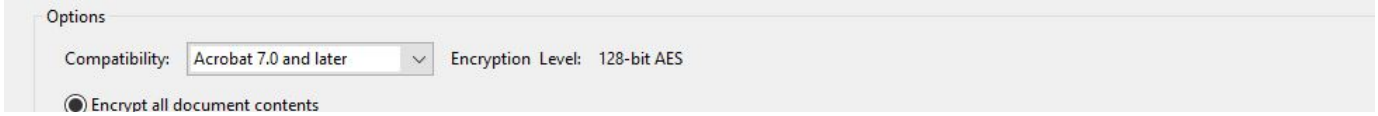


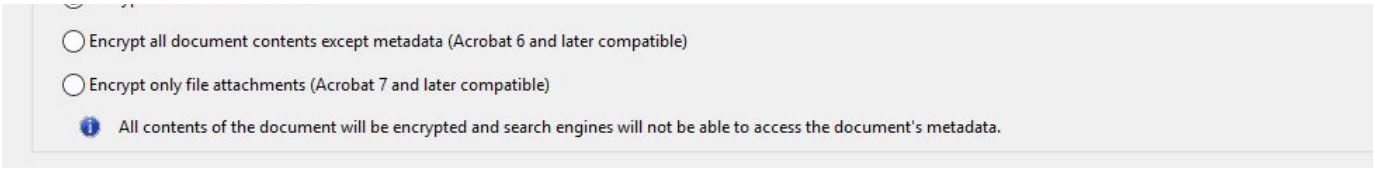
PDF

Signing

Demo

Encrypting





Microsoft Word

Demo

7-Zip

Demo

Wifi Encryption

Thursday, November 16, 2023 4:09 PM

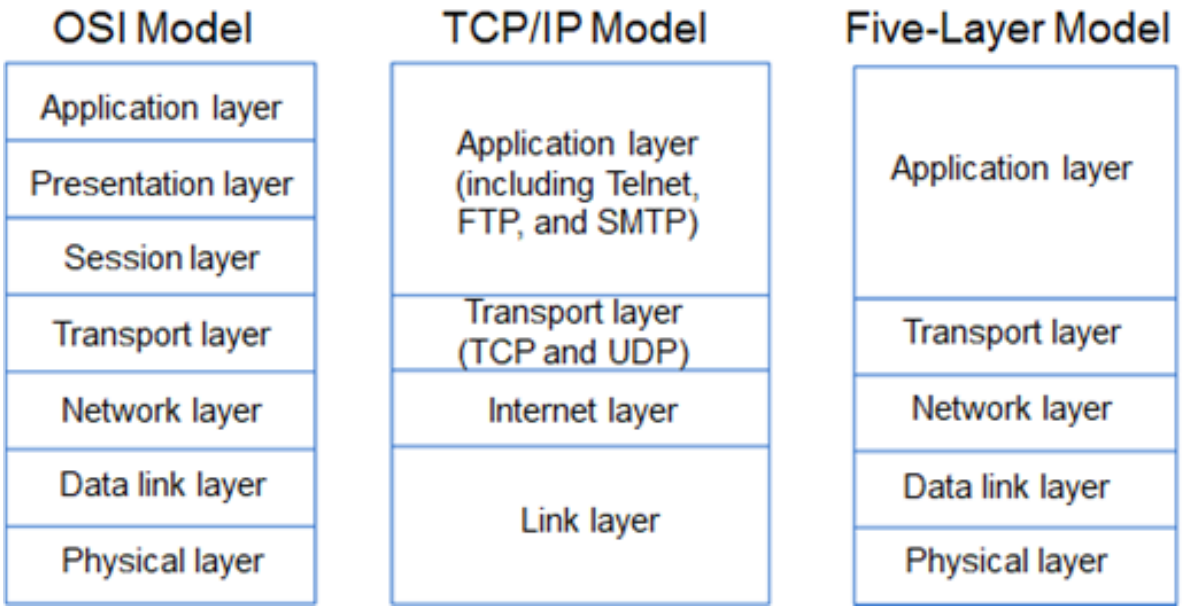
Anouncements:

Don't forget about your book report (and 5 min presentation) due Dec 4th

Why does wifi need to be encrypted?

What layer does this encryption occur?

At what layer has all our encryption so far occurred?

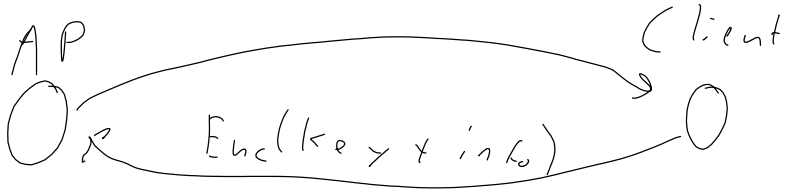


Wifi users have Pre Shared Key (PSK) and need to share this with the Access Point to authenticate.

In the case of a user and a normal server, how is this done?

Why will this meathod not work for wifi?

Information is sent to the user to act as a "salt"



WEP uses RC4 encryption - a stream cipher but the same key (with an IV) is used for every packet

WPA still uses RC4 started using a different key for every packet

WPA2 implemnted AES

We will learn how to break WEP and WPA2

WEP
2 primary weaknesses:

1. Short keys
2. IV resuse

How to break

1. We need to listen to network traffic so our NIC need to be in monitor mode (airmon-ng)
2. We need to record IVs (airodump-ng)

3. We need to use the IVs to crack the key (aircrack-ng)

In practice this is 6 steps:
1. Put NIC in monitor mode (airmon-ng)
2. Scan the network for the AP we want to target (airodump-ng)
3. Monitor specifically the channel you are interested in (airmon-ng)
4. Record the network traffic (airodump-ng)
5. Crack the key (aircrack-ng)
6. Put your NIC back into normal mode (airmon-ng)

Let me demo

Now you try!

WPA2
We will target the "handshake" -> this is how a client authenticates with the AP

Why is this what we target?

How to break:
1. We need to listen to network traffic so our NIC need to be in monitor mode (airmon-ng)
2. We need to record a handshake (airodump-ng)
3. We need perform a dictionary attack to bruteforce the key (aircrack-ng)