Louis Cerda & Finn Dugan
Cpsc 353
Feb 24, 2023

#1.) The best attack would be frequency analysis

#2.) Alice & Bob agree on a encryption/decryption key, however if anyone else knows the key, the whole system fails.

#3.) They face a man in the middle attack.

#4.)

Decrypt(AVFFDDD ADVAXGF)

CENPRTY
AVFFDDD
ADVAXGF

ENCRYPT
V F A D D D
D V A X F G

	A	D	F	G	V	X
A	F	L	1	A	O	Z
D	J	D	ω	3	G	U
F	C	I	Y	B	4	P
G	R	5	ℭ	Ø	V	E
V	6	K	7	z	M	X
X	S	N	H	Ø	T	9

V A D D A F
F D D V X G

7LDG2B

YDOGQJ2

Decrypt(AVFFDDD ADVAXGF)

C	E	N	P	R	T	Y
A	F	D	D	D	A	G
V	F	D	A	V	X	F

Encrypt

F	D	A	D	G	D	A
F	D	V	V	F	A	X

Decrypt text: YDOGQJ2

#10.) $482S + 1180T = \gcd(482, 1180)$

Since by EE $\gcd(482, 1180) = 1$

$482S + 1180T = 1$

$S = 482^{-1}$ of 482 mod 1180

$1180 = 482 \cdot 2 + 216$

$482 = 216 \cdot 2 + 50$

$216 = 50 \cdot 4 + 16$

$50 = 16 \cdot 3 + 2$

$16 = 8 \cdot 2 + 0$

$2 = 50 - 16 \cdot 3$

$= 50 - 3(216 - 50 \cdot 4) = 50 - 3(216) + 3(50 \cdot 4)$

$= 50 - 3(216) + 3(50 \cdot 4)$

$482 - (216 \cdot 2) - 3(216) + 3(50 \cdot 4)$

$482 - (2 \cdot (1180 - (482 \cdot 2))) - 3(216) + 3(50 \cdot 4)$

$482 + 482 \quad - 648 \quad + 600$

$s = 432$

$t = 648$

5.

Division Algorithm

given ints a, b with $b > 0$ $\exists$ unique ints q, r satisfying

$$a = qb + r \quad 0 \leq r < b$$

we say q is the quotient
b is the divisor
r is the remainder

Ex:

$$13 = 4 \cdot 3 + 1$$

6. Use the div alg to show the cube of any int is of the form $9k$, $9k+1$, or $9k+8$

lets consider the cube of an int n

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

n^2 is also an int, so consider the div of n^3 by 9

$n^3 = 9q + r$

by expanding the left-side

$n^3 = n \cdot n^2 = n(9k + r') \equiv 9kn + nr'$

r' is the remainder when n^2 is divided by 9

if we put it back into our equation

$9kn + nr' = 9q + r$

or..

$r = nr' - 9(k-q)$

looking at this we know that r can be any value between 0 and 8, but specific values for n

$0^2 \equiv 0 \pmod 9$
$1^2 \equiv 1 \pmod 9$
$2^2 \equiv 4 \pmod 9$
$3^2 \equiv 0 \pmod 9$
$4^2 \equiv 7 \pmod 9$
$5^2 \equiv 7 \pmod 9$
$6^2 \equiv 0 \pmod 9$
$7^2 \equiv 4 \pmod 9$
$8^2 \equiv 1 \pmod 9$

From this we can see that the possible values of r are 0, 1, 4

If $r' = 0$ then $r = -9(k-q)$, so r is a multiple of 9, therefore can be written as $9k$

If $r' = 1$ then $r = n - 9(k-q)$, so r is 1 more than a multiple of 9, and can be written as $9k+1$

If $r' = 4$ then $r = 4n - 9(k-q)$ so r is 8 more than a multiple of 9 and can be written as $9k+8$

Therefore the cube of any int is of the form $9k$ $9k+1$, or $9k+8$

7. Use the div algorithm to show that the square of any int is of the form $3k$, or $3k+1$

consider the square of an int n

$$n^2 = n \cdot n$$

n is also an int, so lets consider the div of n^2 by 3

$$n^2 = 3q + r$$

expanding the left side we see

$$n^2 = n \cdot n = n(3k + r') \equiv 3kn + r'n$$

r' is the remainder when n is divided by 3

substituting this into our equation we get

$$3kn + r'n = 3q + r$$

or

$$r = r'n - 3(k - q)$$

with this we see that r can be any value between 0 and 2, but n can only take certain values

$0 \equiv 0 \pmod 3$
$1 \equiv 1 \pmod 3$
$2 \equiv 2 \pmod 3$

from this we see that the possible values of r' are 0 or 1 so we consider the values of r

if $r' = 0$ then $r = -3(k-q)$ so r is a multiple of 3 and is written as $3k$

if $r' = 1$ then $r = n - 3(k-q)$ so r is 1 more than a multiple of 3 and can be written as $3k+1$

8. Show that $3a^2-1$ is never a perfect square

Suppose, for the sake of contradiction that there exists an int a, such that $3a^2-1$ is a perfect square. We can then write:

$3a^2-1=b^2$ where b is an int. By adding 1 to both sides we get $3a^2=b^2+1$

Using the result from 7, b^2+1 must be of the form $3k$ or $3k+1$ for some int k. But this is a contradiction, since the left-hand side of the equation is always of the form $3a^2$ for any int a.

Therfore, $3a^2-1$ can never be a perfect square

9. $1180 = 2 \cdot 482 + 216$

$216 = 1180 - 2 \cdot 482$

$482 = 2 \cdot 216 + 50$

$50 = 482 - 2 \cdot 216$

$= 482 - 2(1180 - 2 \cdot 482)$

$= -5 \cdot 1180 + 12 \cdot 482$

$216 = 4 \cdot 50 + 16$

$16 = 216 - 4 \cdot 50$

$= 9 \cdot 1180 - 22 \cdot 482$

$\gcd(1180, 482) = 16$