

Sean Poston

MA464

Exam 1

Exam 1

Sean Poston

$$1. \gcd(5678, 1234) \rightarrow 1234 \cdot 4 + 742$$

$$\gcd(1234, 742) \rightarrow 742 \cdot 1 + 492$$

$$\gcd(742, 492) \rightarrow 492 \cdot 1 + 250$$

$$\gcd(492, 250) \rightarrow 250 \cdot 1 + 242$$

$$\gcd(250, 242) \rightarrow 242 \cdot 1 + 8$$

$$\gcd(242, 8) \rightarrow 8 \cdot 30 + 2$$

$$\gcd(8, 2) \rightarrow 2 \cdot 4 + 0$$

$$\boxed{\gcd = 2}$$

1234 would not have a multiplicative inverse because the $\gcd \neq 1$.

Sean Poston

MA464

Exam 1

$$2. \quad 10! = 3,628,800 \quad \phi(10!)$$

$$\phi(2 \cdot 3 \cdot 2^2 \cdot 5 \cdot (3 \cdot 2) \cdot 7 \cdot 2^3 \cdot 3^2 \cdot (5 \cdot 2))$$

$$\phi(2^6 \cdot 3^3 \cdot 5 \cdot (3 \cdot 2) \cdot 7 \cdot (5 \cdot 2))$$

$$\phi(2^8 \cdot 3^4 \cdot 5^2 \cdot 7)$$

$$\phi(2^8) \cdot \phi(3^4) \cdot \phi(5^2) \cdot \phi(7)$$

$$(2^8 - 2^7) \cdot (3^4 - 3^3) \cdot (5^2 - 5) \cdot (7 - 1)$$

$$(128) \cdot (54) \cdot 20 \cdot 6 = \boxed{829,440}$$

Sean Poston

MA464

Exam 1

3. $\begin{bmatrix} 15 & 24 & 1 \\ 7 & 3 & 0 \\ 17 & 0 & 16 \end{bmatrix}_{3 \times 3}$ $\det = -2019$
 $\gcd(\det, 26) = 1$
This why the matrix is invertible.

4. K V N T D F \rightarrow 10 21 13 19 3 5
- finish \rightarrow 5 8 13 8 18 7
Key \rightarrow 5 13 0 11 11 24 pt 2 = The end
Y U E P Y B \rightarrow 24 20 4 15 24 1 Key = F N A L L Y
- Key \rightarrow 5 13 0 11 11 24
T H E E N D

Sean Poston

MA464

Exam 1

5. random # $y, z \in \mathbb{Z}_{26}$

$$(3 \cdot 7 + 6) \mod 26 = 1$$

$$(8 \cdot 7 + 6) \mod 26 = 10$$

not invertible

$$(1 \cdot 15 + 10) \mod 26 = 25$$

$$(10 \cdot 15 + 10) \mod 26 = 4$$

$$15 \cdot 7 + 6 = 7$$

$$23 \cdot 7 + 6 = 10$$

$$7 \cdot 15 + 10 = 11$$

$$10 \cdot 15 + 10 = 14$$

$$25 \rightarrow 21$$

$$(15 \cdot 14 + 9) \mod 26 = 11$$

$$(23 \cdot 14 + 9) \mod 26 = 19$$

$$e_k(x) = (a, b) \Rightarrow (14, 9)$$

Part 2

$$A = \begin{bmatrix} 14 & 19 & 22 \\ 0 & 12 & 21 \\ 13 & 22 & 2 \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} 14 & 14 & 11 \\ 13 & 20 & 24 \\ 0 & 1 & 16 \end{bmatrix}$$

$$\text{ctm: } \begin{bmatrix} 6 & 1 & 17 \\ 6 & 15 & 20 \\ 4 & 14 & 6 \\ 6 & 19 & 16 \\ 22 & 10 & 12 \\ \vdots & \vdots & \vdots \end{bmatrix}$$

$$\cdot A^{-1} \cdot 26 \Rightarrow$$

$$\begin{bmatrix} 19 & 17 & 24 \\ 19 & 14 & 18 \\ 4 & 4 & 8 \\ 19 & 12 & 24 \\ 22 & 0 & 24 \\ \vdots & \vdots & \vdots \end{bmatrix}$$

$$\xrightarrow{\text{nttc}}$$

$$\begin{bmatrix} t & o & w \\ e & c & k \\ t & m & u \\ w & a & k \\ \vdots & \vdots & \vdots \end{bmatrix}$$

The plaintext is the Beatles' "We Can Work It Out"

Cipher Text: |

GBRGPU EOGGTQWKMLMHXOE OV KOAPLATFYXAYGYBYXVPMSGNAOWBHDGEWWUIURSIYY

Cipher Text Matrix Numbers:

[[6, 1, 17], [6, 15, 20], [4, 14, 6], [6, 19, 16], [22, 10, 12],

Plain Text Matrix Numbers:

[[19 17 24]

[19 14 18]

[4 4 8]

[19 12 24]

[22 0 24]

Plain Text:

TRYTOSEEITMYWAYDOIHAVETOKEEPONTALKINGTILLICANTGOONWHILEYOUSEEITYO

TRY TO SEE IT MY WAY.

DO I HAVE TO KEEP ON TALKING 'TILL I CAN'T GO ON WHILE YOU SEE IT YOUR WAY?

RUN THE RISK OF KNOWING THAT OUR LOVE MAY SOON BE GONE.

WE CAN WORK IT OUT. WE CAN WORK IT OUT.

THINK OF WHAT YOU'RE SAYING.

YOU CAN GET IT WRONG, AND STILL YOU THINK THAT IT'S ALRIGHT.

THINK OF WHAT I'M SAYING.

WE CAN WORK IT OUT AND GET IT STRAIGHT OR SAY GOODNIGHT.

WE CAN WORK IT OUT. WE CAN WORK IT OUT.

LIFE IS VERY SHORT, AND THERE'S NO TIME FOR FUSSING AND FIGHTING, MY FRIEND.

I HAVE ALWAYS THOUGHT THAT IT'S A CRIME, SO I WILL ASK YOU ONCE AGAIN.

AND NOW MY LIFE HAS CHANGED IN OH SO MANY WAYS.

MY INDEPENDENCE SEEMS TO VANISH IN THE HAZE, BUT EVERY NOW AND THEN I FEEL SO INSECURE.

I KNOW THAT I JUST NEED YOU LIKE I'VE NEVER DONE BEFORE.

HELP ME IF YOU CAN; I'M FEELING DOWN, AND I DO APPRECIATE YOU BEING ROUND.

HELP ME GET MY FEET BACK ON THE GROUND.

WON'T YOU PLEASE, PLEASE HELP ME.

WHEN I WAS YOUNGER, SO MUCH YOUNGER THAN TODAY, I NEVER NEEDED ANYBODYS HELP IN ANY WAY.

BUT NOW THESE DAYA ARE GONE.

I'M NOT SO SELF-ASSURED NOW.

IF IN D I'VE CHANGED MY MIND AND OPENED UP THE DOORS.

HELP ME IF YOU CAN I'M FEELING DOWN, AND I DO APPRECIATE YOU BEING ROUND.

HELP ME GET MY FEET BACK ON THE GROUND.

WON'T YOU PLEASE, PLEASE HELP ME. HELP ME. HELP ME, OH.

DO YOU RECOGNIZE THE PLAINTEXT?

Q