2. Prove that if n is even, then 10n-2 is even.

3. Prove that if n is even, then n*n+n is even.

4. Prove that if n*n is even then n is even.

5. Prove that if n*n is odd then n is odd.

6. Prove (for all integers a, x and y) that if a|x and a|y then a|(2*x-3*y).

Points 100

Submitting Nothing

Due	For	Available from	Until
Oct 22 at 12pm	Everyone	-	-

+ Rubric

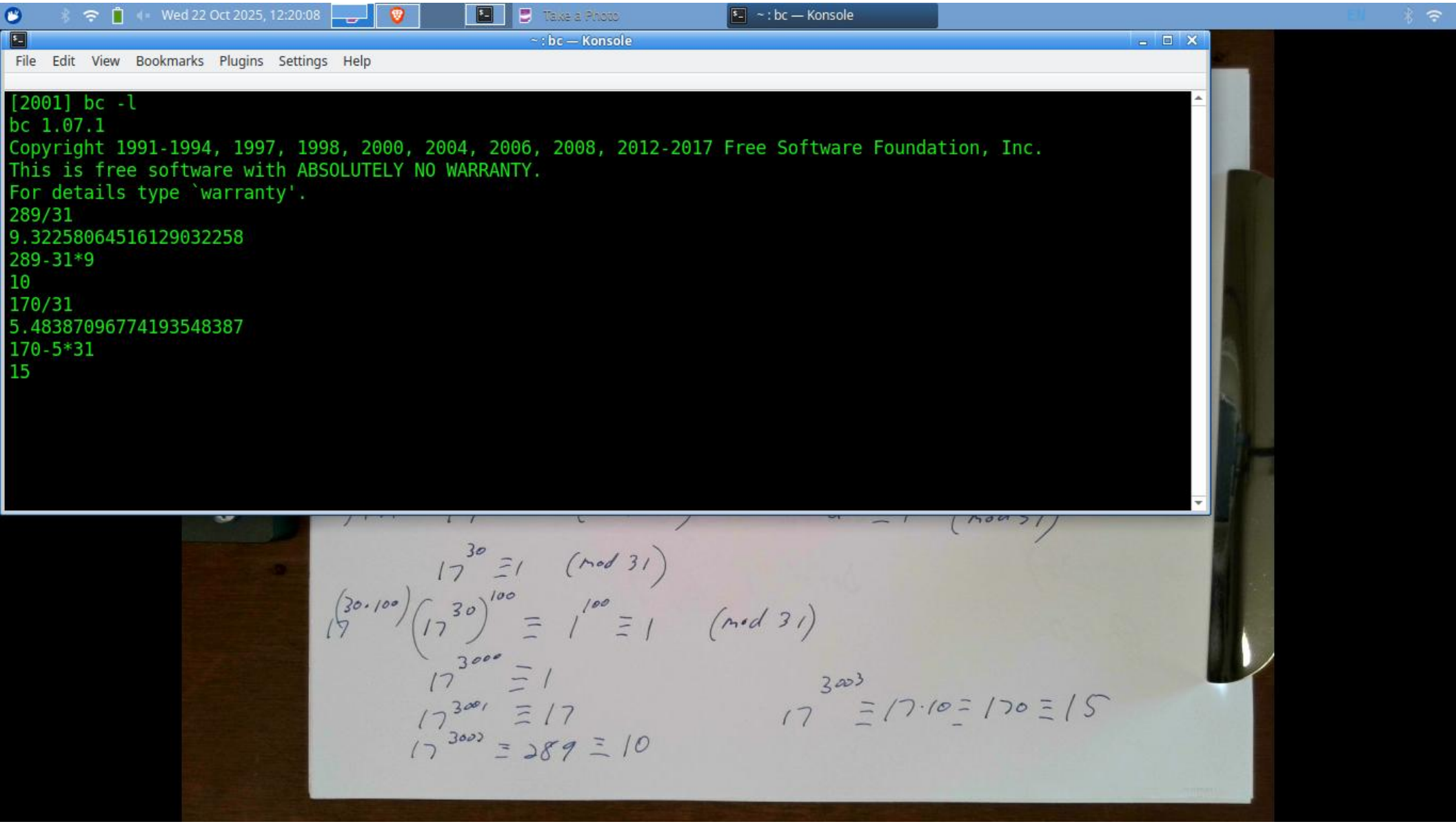
◂ Previous

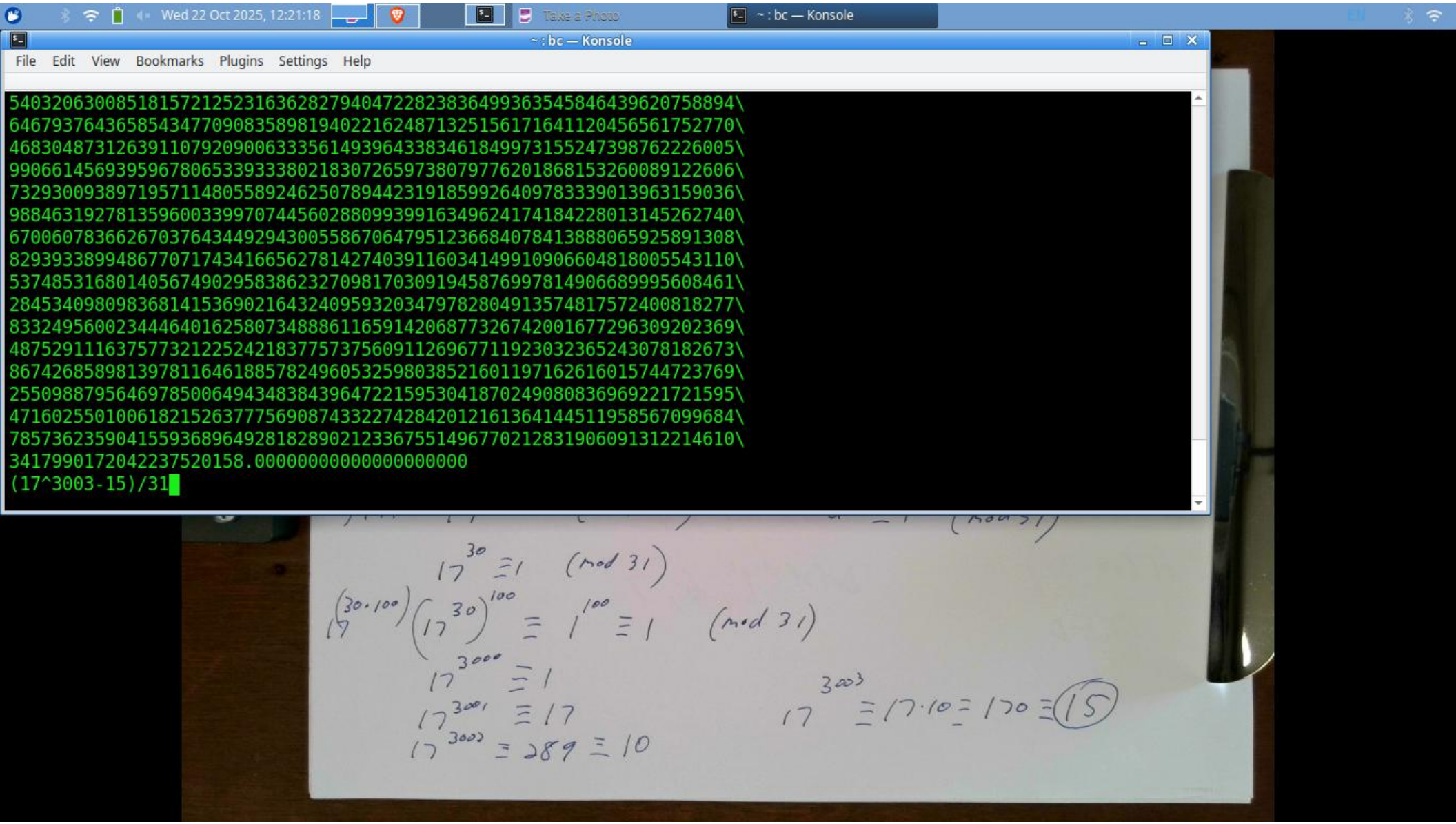
Next ▸

Prove if $a|x$ and $a|y$ then $a|(2x-3y)$

1. $a|x$ Hyp
2. $a|y$ Hyp
3. $\exists k \in \mathbb{Z}: x = ak$ Def of "|", 1.
4. $\exists j \in \mathbb{Z}: y = aj$ Def of "|", 2.
5. $2x-3y = 2 \cdot ak - 3aj$ Subs, 3, 4
6. $2x-3y = a(2k-3j)$ factor out a
7. $2k-3j \in \mathbb{Z}$ closure of ints, 3, 4
8. $a|(2x-3y)$ Def of "|", 6, 7

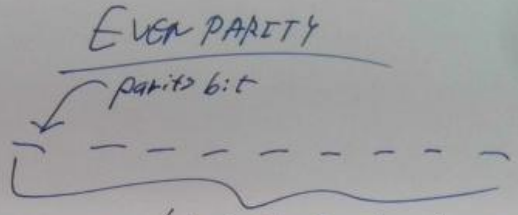
QED


Wed 22 Oct 2025, 12:20:08
Take a Photo
~ : bc — Konsole
~ : bc — Konsole
File Edit View Bookmarks Plugins Settings Help
[2001] bc -l
bc 1.07.1
Copyright 1991-1994, 1997, 1998, 2000, 2004, 2006, 2008, 2012-2017 Free Software Foundation, Inc.
This is free software with ABSOLUTELY NO WARRANTY.
For details type `warranty'.
289/31
9.32258064516129032258
289-31*9
10
170/31
5.48387096774193548387
170-5*31
15
17^30 ≡ 1 (mod 31)
17^(30·100) (17^30)^100 ≡ 1^100 ≡ 1 (mod 31)
17^3000 ≡ 1
17^3001 ≡ 17
17^3002 ≡ 289 ≡ 10
17^3003 ≡ 17·10 ≡ 170 ≡ 15


Wed 22 Oct 2025, 12:21:18
Take a Photo
~ : bc — Konsole
~ : bc — Konsole
File Edit View Bookmarks Plugins Settings Help
5403206300851815721252316362827940472282383649936354584643962075889 4\
6467937643658543477090835898194022162487132515617164112045656175277 0\
4683048731263911079209006333561493964338346184997315524739876222600 5\
9906614569395967806533933380218307265973807977620186815326008912260 6\
7329300938971957114805589246250789442319185992640978333901396315903 6\
9884631927813596003399707445602880993991634962417418422801314526274 0\
6700607836626703764344929430055867064795123668407841388806592589130 8\
8293933899486770717434166562781427403911603414991090660481800554311 0\
5374853168014056749029583862327098170309194587699781490668999560846 1\
2845340980983681415369021643240959320347978280491357481757240081827 7\
8332495600234446401625807348886116591420687732674200167729630920236 9\
4875291116375773212252421837757375609112696771192303236524307818267 3\
8674268589813978116461885782496053259803852160119716261601574472376 9\
2550988795646978500649434838439647221595304187024908083696922172159 5\
4716025501006182152637775690874332274284201216136414451195856709968 4\
7857362359041559368964928182890212336755149677021283190609131221461 0\
3417990172042237520158.000000000000000000
(17^3003-15)/31
$17^{30} \equiv 1 \pmod{31}$
$17^{30 \cdot 100} = (17^{30})^{100} \equiv 1^{100} \equiv 1 \pmod{31}$
$17^{3000} \equiv 1$
$17^{3001} \equiv 17$
$17^{3002} \equiv 289 \equiv 10$
$17^{3003} \equiv 17 \cdot 10 \equiv 170 \equiv 15$

Parity

EVEN PARITY



H L L H L H H L

0 1 0 0 0 0 0 1 'A'

L H L L L L H H

0 1 0 0 0 0 1 1 'G'

0 0 0 0 0 0 0 0

ODD PARITY

total # of 1's is odd

1 0 0 0 0 0 0 0

ECC Memory

Hash functions (MD5)

UPC 11 digits + check digit

$d_0\ d_1\ d_2\ \ldots\ d_{11}$

$S = 3d_0 + d_1 + 3d_2 + d_3 + \ldots + 3d_{10} + d_{11} \pmod{10}$

If $S \neq 0$, $S = 10 - S$

ISBN

CRYPTOGRAPHY

Caesar Cipher

A → X
B → D
C → W
D → A
.
.
.

encode: turn plain text into cypher text

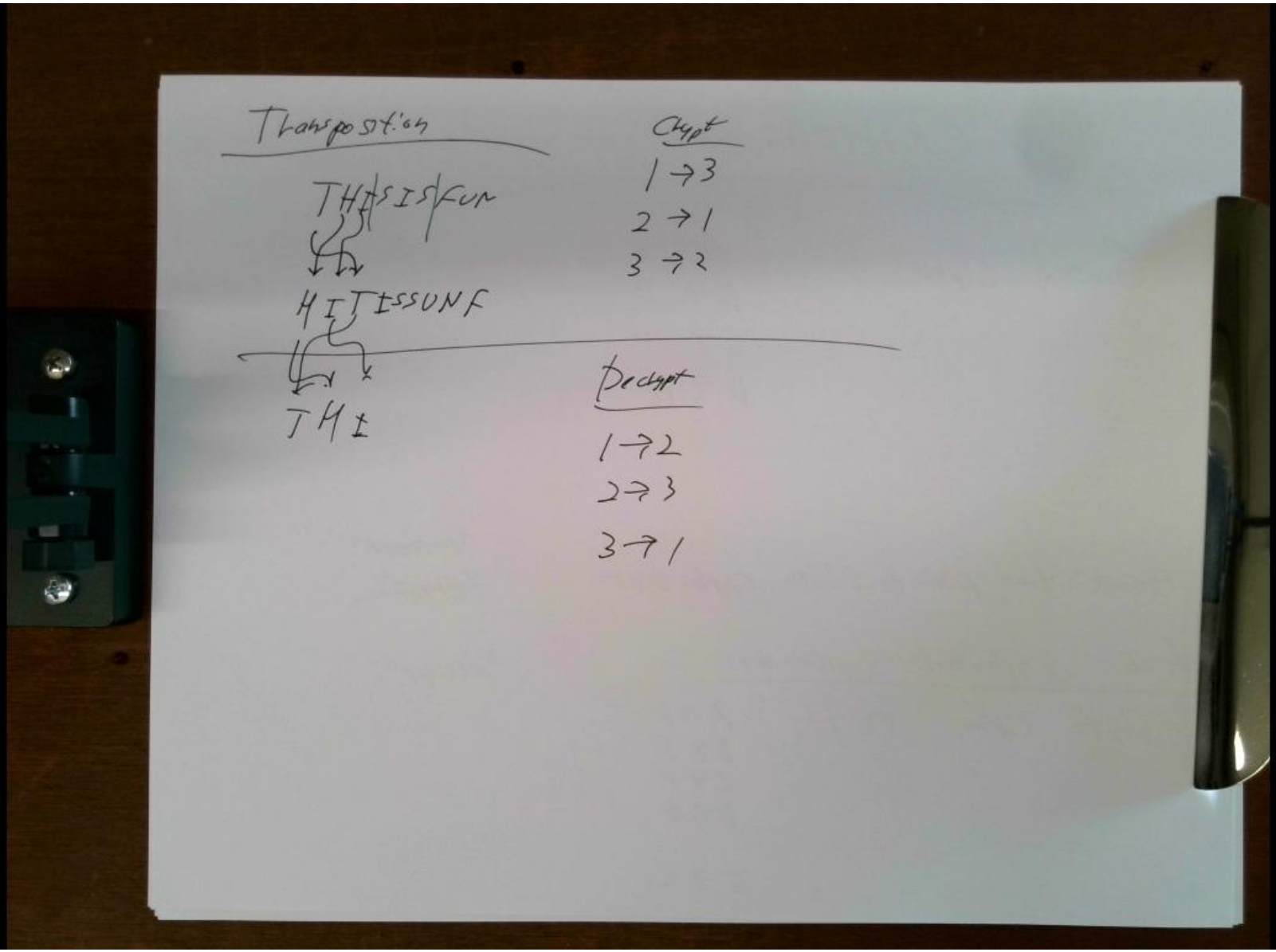
decode: cypher text → plain text

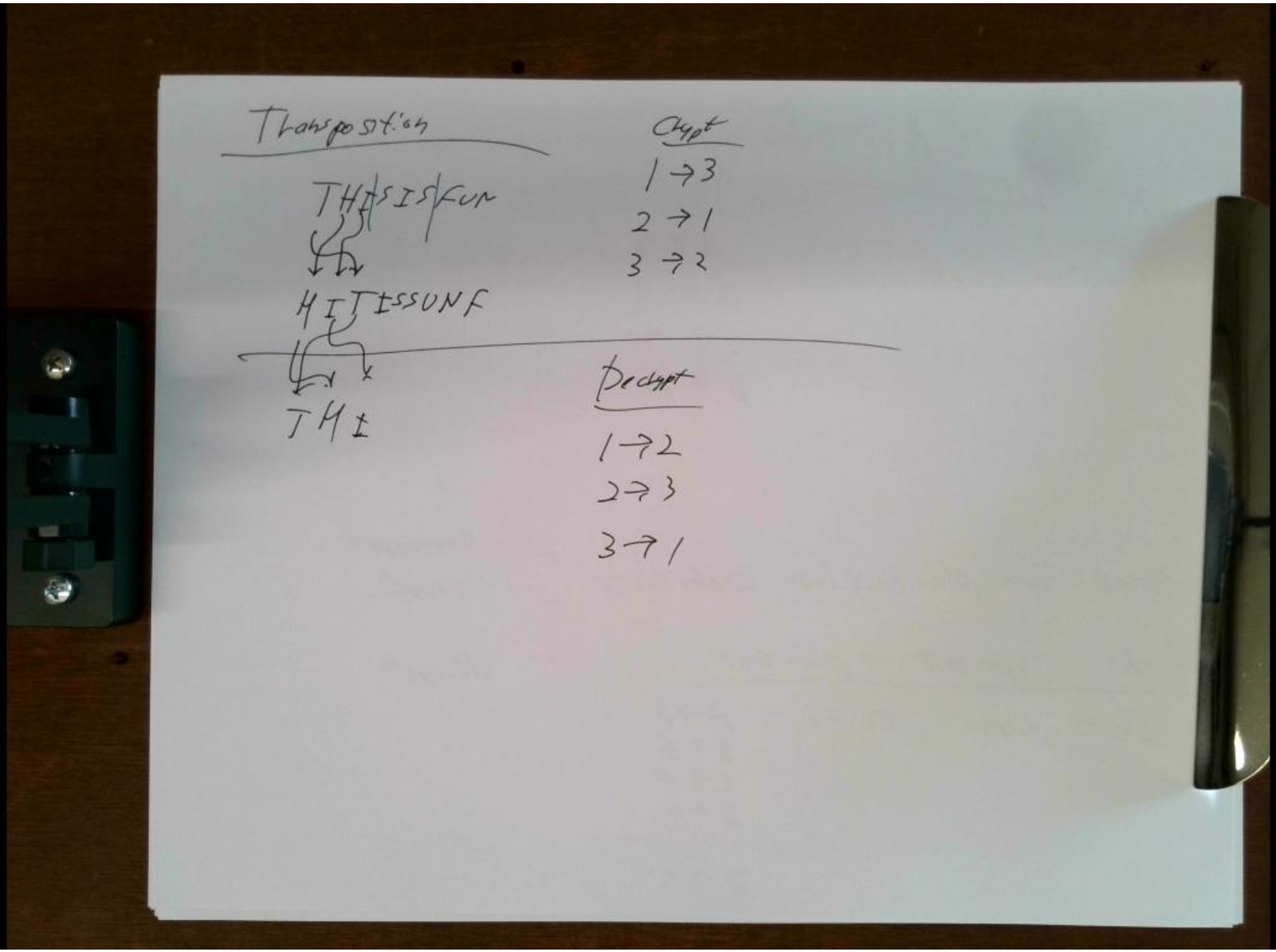
"encrypt"
~~"crypt"~~

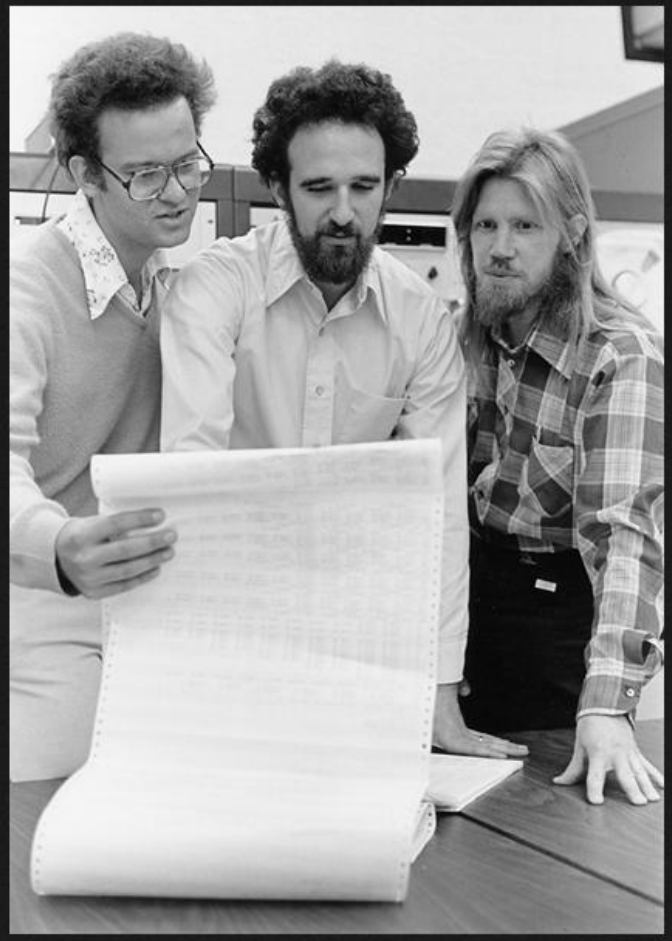
"decrypt"

Shift cipher: ex: +3

A → D
B → E
C → F
D → G
.
.
.
Z → C


Transposition
THISISFUN
HITISSUNF
THI
Crypt
1→3
2→1
3→2
Decrypt
1→2
2→3
3→1


Transposition
THISISFUN
HITISSUNF
THI
Crypt
1→3
2→1
3→2
Decrypt
1→2
2→3
3→1



DES

A Symmetric cypher uses the same* password for encryption & decryption

* Or, if you know how to encrypt, you can easily figure out how to decrypt.

---

an Asymmetric cypher uses different keys:

If you know how to encrypt, you still can't figure out how to decrypt.

Public key : encrypt

Private key : decrypt

RSA

pick 2 large primes p, q $\quad n = p \cdot q$

find a number e relatively prime to $(p-1)(q-1)$

Encryption key: (n, e)

How to encrypt $\quad A = 00,\ B = 01,\ C = 02,\ \ldots,\ Z = 25$

HELLO → 07 04 11 11 15

Break into blocks of characters so

$$\underbrace{25252525\ldots25}_{2N \text{ chars}} < n$$

Message: M

If you know p & q, you can find a d : $de \equiv 1 \mod (p-1)(q-1)$

relatively prime to $(p-1)(q-1)$

Encryption key: (n, e)

How to encrypt $A=00$, $B=01$, $C=02$, $\ldots$, $Z=25$

Hello → 07040111115

Break into blocks of characters so

$$\underbrace{25252525\ldots25}_{2N \text{ chars}} < n$$

Message: M

If you know p & q, you can find a d : $de \equiv 1 \pmod{(p-1)(q-1)}$

To encrypt, just do $M^e \pmod{n}$

C "

DECRYPT

$de \equiv 1 \pmod{(p-1)(q-1)}$

So $\exists k \in \mathbb{Z}$: $de = k(p-1)(q-1) + 1$

$n = p \cdot q$

$$C^d \equiv (M^e)^d \equiv M^{de} \equiv M^{k(p-1)(q-1)+1} \pmod{n}$$

$$C^d \equiv M^{k(p-1)(q-1)+1} \pmod{p}$$

$$\equiv M^{k(p-1)(q-1)\times 1} \pmod{q}$$

Assume $GCD(M, p) \equiv GCD(M, q) = 1$

FLT: $M^{p-1} \equiv 1 \pmod{p}$

$$C^d \equiv M^{(p-1)k(q-1)+1} \equiv M^{(p-1)(k)(q-1)} \equiv 1^{k(q-1)} \equiv 1 \pmod{p}$$

$$\equiv M \pmod{p}$$

$C^d \equiv M \pmod{p}$ $\quad GCD(p,q) = 1$

$C^d \equiv M \pmod{q}$

$\therefore$ by Chinese Remainder Theorem

$$C^d \equiv M \pmod{p \cdot q}$$
$$\pmod{n}$$

Decryption key: (d, n)

$C^d \equiv M \pmod{p}$ $\quad GCD(p,q) = 1$

$C^d \equiv M \pmod{q}$

$\therefore$ by Chinese Remainder Theorem

$$C^d \equiv M \pmod{p \cdot q}$$
$$\pmod{n}$$

Decryption key: (d, n)