Cryptography Engineering Quiz 1

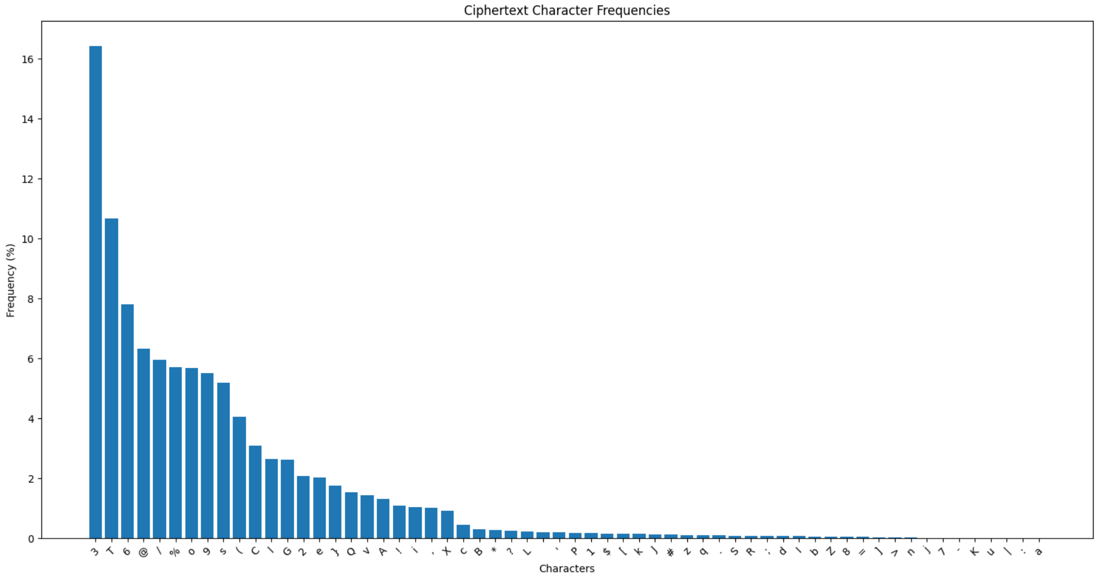
111511157 黃湇琪

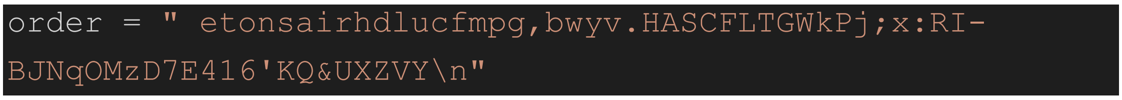
Problem 1

a)

Table 1: Ciphertext-to-plaintext mapping (ASCII 32–126)

Ciphertext	(space)	!	"	#	$	%	&	'	(	)	*	+	,	-	.
ASCII	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
Plaintext	F	b		;	W	s		L	h		A		y	6	R
Ciphertext	/	0	1	2	3	4	5	6	7	8	9	:	;	<	=
ASCII	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61
Plaintext	n		G	c	space		t	l	M	i	&	B		z	
Ciphertext	>	?	@	A	B	C	D	E	F	G	H	I	J	K	L
ASCII	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76
Plaintext	7	S	o	,	H	d				u		N	j	‘	C
Ciphertext	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	[
ASCII	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91
Plaintext				T	p	-	I	e				v		O	k
Ciphertext	\	]	^	_	`	a	b	c	d	e	f	g	h	i	j
ASCII	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106
Plaintext		D				U	q	.	J	f				w	4
Ciphertext	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
ASCII	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121
Plaintext	P	l		E	a		:		r		K	g			
Ciphertext	z	{	|	}	~										
ASCII	122	123	124	125	126										
Plaintext	x		Q	m											



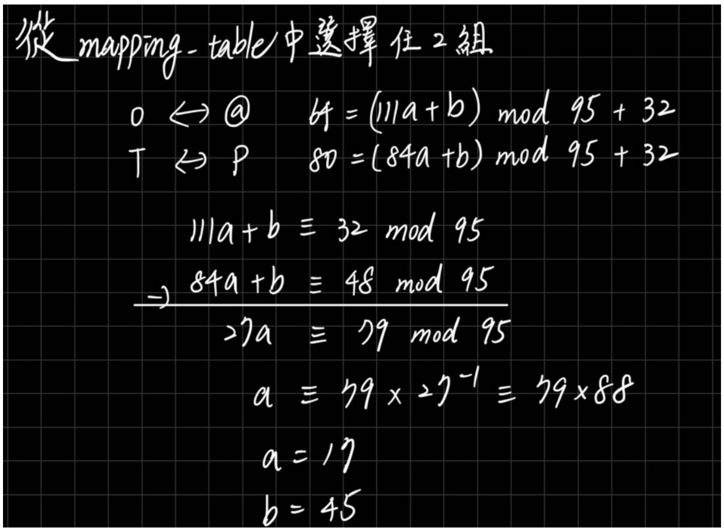


```
order = " etonsairhdlucfmpg,bwyv.HASCFLTGWkPj;x:RI-
BJNqOMzD7E416'KQ&UXZVY\n"
```

In Congress, July 4, 1776. The unanimous Declaration of the thirteen united States of America, When in the Course of human events, it becomes necessary for one people to dissolve the political bands which have connected them with another, and to assume among the powers of the earth, the separate and equal station to which the Laws of Nature and of Nature's God entitle them, a decent respect to the opinions of mankind requires that they should declare the causes which impel them to the separation. We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.--That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed, --That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness. Prudence, indeed, will dictate that Governments long established should not be changed for light and transient causes; and accordingly all experience hath shewn, that mankind are more disposed to suffer, while evils are sufferable, than to right themselves by abolishing the forms to which they are accustomed. But when a long train of abuses and usurpations, pursuing invariably the same Object evinces a design to reduce them under absolute Despotism, it is their right, it is their duty, to throw off such Government, and to provide new Guards for their future security.--Such has been the patient sufferance of these Colonies; and such is now the necessity which constrains them to alter their former Systems of Government. The history of the present King of Great Britain is a history of repeated injuries and usurpations, all having in direct object the establishment of an absolute Tyranny over these States. To prove this, let Facts be submitted to a candid world. He has refused his Assent to Laws, the most wholesome and necessary for the public good. He has forbidden his Governors to pass Laws of immediate and pressing importance, unless suspended in their operation till his Assent should be obtained; and when so suspended, he has utterly neglected to attend to them. He has refused to pass other Laws for the accommodation of large districts of people, unless those people would relinquish the right of Representation in the Legislature, a right inestimable to them and formidable to tyrants only. He has called together legislative bodies at places unusual, uncomfortable, and distant from the depository of their public Records, for the sole purpose of fatiguing them into compliance with his measures. He has dissolved Representative Houses repeatedly, for opposing with manly firmness his invasions on the rights of the people. He has refused for a long time, after such dissolutions, to cause others to be elected; whereby the Legislative powers, incapable of Annihilation, have returned to the People at large for their exercise; the State remaining in the mean time exposed to all the dangers of invasion from without, and convulsions within. He has endeavoured to prevent the population of these States; for that purpose obstructing the Laws for Naturalization of Foreigners; refusing to pass others to encourage their migrations hither, and raising the conditions of new Appropriations of Lands. He has obstructed the Administration of Justice, by refusing his Assent to Laws for establishing Judiciary powers. He has made Judges dependent on his Will alone, for the tenure of their offices, and the amount and payment of their salaries. He has erected a multitude of New Offices, and sent hither swarms of Officers to harrass our people, and eat out their substance. He has kept among us, in times of peace, Standing Armies without the

Consent of our legislatures. He has affected to render the Military independent of and superior to the Civil power. He has combined with others to subject us to a jurisdiction foreign to our constitution, and unacknowledged by our laws; giving his Assent to their Acts of pretended Legislation: For Quartering large bodies of armed troops among us: For protecting them, by a mock Trial, from punishment for any Murders which they should commit on the Inhabitants of these States: For cutting off our Trade with all parts of the world: For imposing Taxes on us without our Consent: For depriving us in many cases, of the benefits of Trial by Jury: For transporting us beyond Seas to be tried for pretended offences For abolishing the free System of English Laws in a neighbouring Province, establishing therein an Arbitrary government, and enlarging its Boundaries so as to render it at once an example and fit instrument for introducing the same absolute rule into these Colonies: For taking away our Charters, abolishing our most valuable Laws, and altering fundamentally the Forms of our Governments: For suspending our own Legislatures, and declaring themselves invested with power to legislate for us in all cases whatsoever. He has abdicated Government here, by declaring us out of his Protection and waging War against us. He has plundered our seas, ravaged our Coasts, burnt our towns, and destroyed the lives of our people. He is at this time transporting large Armies of foreign Mercenaries to compleat the works of death, desolation and tyranny, already begun with circumstances of Cruelty & perfidy scarcely paralleled in the most barbarous ages, and totally unworthy the Head of a civilized nation. He has constrained our fellow Citizens taken Captive on the high Seas to bear Arms against their Country, to become the executioners of their friends and Brethren, or to fall themselves by their Hands. He has excited domestic insurrections amongst us, and has endeavoured to bring on the inhabitants of our frontiers, the merciless Indian Savages, whose known rule of warfare, is an undistinguished destruction of all ages, sexes and conditions. In every stage of these Oppressions We have Petitioned for Redress in the most humble terms: Our repeated Petitions have been answered only by repeated injury. A Prince whose character is thus marked by every act which may define a Tyrant, is unfit to be the ruler of a free people. Nor have We been wanting in attentions to our Brittish brethren. We have warned them from time to time of attempts by their legislature to extend an unwarrantable jurisdiction over us. We have reminded them of the circumstances of our emigration and settlement here. We have appealed to their native justice and magnanimity, and we have conjured them by the ties of our common kindred to disavow these usurpations, which, would inevitably interrupt our connections and correspondence. They too have been deaf to the voice of justice and of consanguinity. We must, therefore, acquiesce in the necessity, which denounces our Separation, and hold them, as we hold the rest of mankind, Enemies in War, in Peace Friends. We, therefore, the Representatives of the united States of America, in General Congress, Assembled, appealing to the Supreme Judge of the world for the rectitude of our intentions, do, in the Name, and by Authority of the good People of these Colonies, solemnly publish and declare, That these United Colonies are, and of Right ought to be Free and Independent States; that they are Absolved from all Allegiance to the British Crown, and that all political connection between them and the State of Great Britain, is and ought to be totally dissolved; and that as Free and Independent States, they have full Power to levy War, conclude Peace, contract Alliances, establish Commerce, and to do all other Acts and Things which Independent States may of right do. And for the support of this Declaration, with a firm reliance on the protection of divine Providence, we mutually pledge to each other our Lives, our Fortunes and our sacred Honor.

b) a=17, b=45



從 mapping-table 中選擇任2組

$0 \leftrightarrow @ \quad 64 = (111a+b) \bmod 95 + 32$

$T \leftrightarrow P \quad 80 = (84a+b) \bmod 95 + 32$

$$\begin{array}{rl} & 111a+b \equiv 32 \bmod 95 \\ -) & 84a+b \equiv 48 \bmod 95 \\ \hline & 27a \equiv 79 \bmod 95 \end{array}$$

$a \equiv 79 \times 27^{-1} \equiv 79 \times 88$

$a = 17$

$b = 45$

c) The attacker can use the **known plaintext attack (KPA)** technique to break the encryption. Since the word "created" is known to exist in the plaintext, the corresponding ciphertext can be identified. This provides multiple plaintext-ciphertext pairs that can be used to solve for the encryption parameters. Specifically, since the affine cipher follows the formula y=(ax+b)mod 95+32, knowing multiple values of x (plaintext characters) and their corresponding y (ciphertext characters) allows the attacker to set up a system of linear congruences. By solving these equations, the attacker can determine the values of a and b, effectively breaking the encryption.

d) The size of the key space for the affine cipher is determined by the number of valid a values and the number of possible b values.
Since a must be coprime to 95 (i.e., gcd(a,95)=1), the number of valid choices for a is given by Euler's totient function ϕ(95), which is 72. The parameter b can be any value from 0 to 94, giving 95 possible choices. Therefore, the total key space size is **72×95=6840**.

This is relatively small compared to more secure encryption methods. The affine cipher is weak because its key space can be easily exhausted via brute force, and it preserves frequency distributions, making it highly vulnerable to frequency analysis.

e) A monoalphabetic substitution cipher over the ASCII range from 32 to 126 has a much larger key space since it allows for any permutation of 95 characters. The number of possible keys is given by **95!** (95 factorial), which is an extremely large number, making brute-force attacks practically infeasible. However, this cipher is still vulnerable to frequency analysis because the character mappings remain fixed throughout the text. If an attacker has enough ciphertext, they can compare letter frequencies to standard distributions of English text to deduce the substitution pattern.

f) A modular affine transformation followed by a transposition step.

- Step 1: Affine Transformation with Modulo 95
  The plaintext character x (ASCII 32–126) is first transformed using an affine function: y=(ax+b) mod 95+32
  This ensures that the mapping is invertible while spreading out frequency distributions.

- Step 2: Block-Based Transposition Permutation
  The resulting intermediate ciphertext is then subjected to a block-based transposition. The message is divided into blocks of a fixed size (e.g., 4, 8, or 16 characters), and a predetermined key-dependent permutation is applied within each block. For example, if the block size is 4 and the key specifies a permutation of [3,1,4,2], then:

  - The 1st character moves to the 3rd position.
  - The 2nd character moves to the 1st position.
  - The 3rd character moves to the 4th position.
  - The 4th character moves to the 2nd position.

➢ How This Meets the Criteria

- Includes at least two transformation steps: The combination of an affine transformation and a transposition ensures that frequency-based attacks are mitigated.
- Makes frequency analysis more difficult: Since transposition disrupts the relative positions of characters, frequency analysis alone cannot directly reveal letter substitutions. An attacker would first need to undo the transposition step before analyzing character frequencies.
- Fully reversible for accurate decryption: Decryption follows the reverse process. First, the transposition is undone using the inverse permutation, and then the affine transformation is reversed using modular arithmetic, applying: $x=a^{-1}(y-b) \bmod 95$ where a^{-1} is the modular inverse of a modulo 95.

➢ Example

Plaintext: HELLO WORLD!

1. Affine Transformation：Bn"Z3$Z.']D
2. Block-Based Transposition(Block size: 4, order: [2, 0, 3, 1]) : 'B'n$ZZ3].D'

Problem 2

a)

1. Number of valid values for a:
   Since n is prime, every number $a \in \{1,2,...,n-1\}$ is coprime to n, so there are $\varphi(n)=n-1$ choices for a.
2. Number of possible values for b:
   Since b can take any value in $\{0,1,...,n-1\}$, there are n choices.
3. Total number of keys:
   The total number of keys is: **$(n-1)\times n$**

Since n is prime and within the range 30<n<100, the exact key space size depends on the specific value of n.

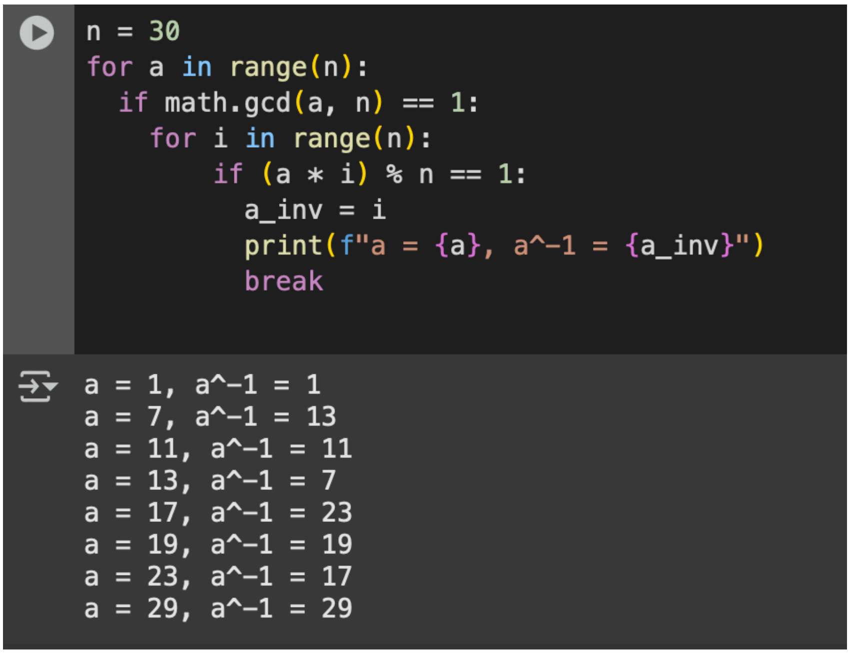
n	31	37	41	43	47	53	59	61	67
size	930	1332	1640	1806	2162	2756	3422	3660	4422

n	71	73	79	83	89	97
size	4970	5256	6162	6806	7832	9312

b)

gcd(a,30)=1 means any number not divisible by 2, 3, or 5 is coprime to 30.

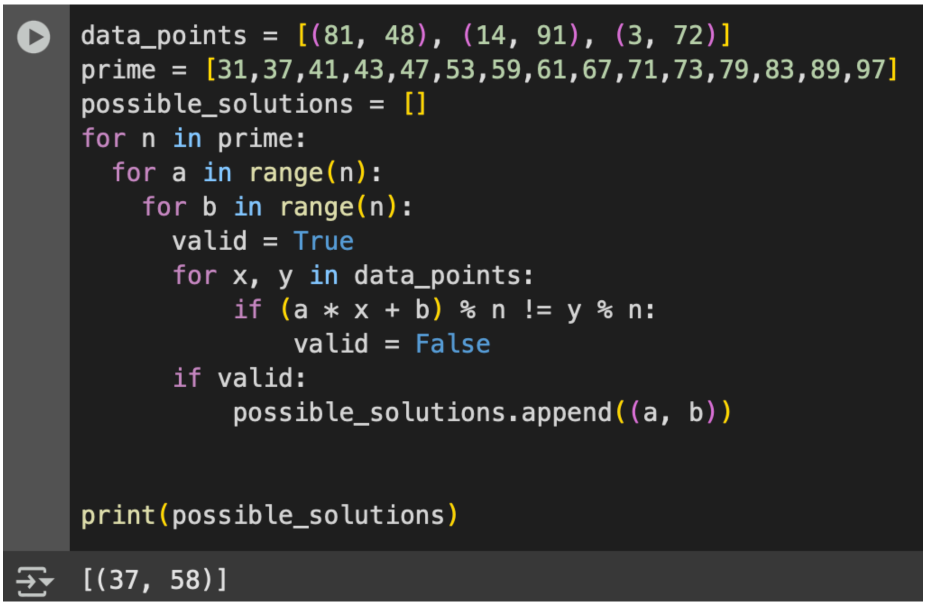
a	1	7	11	13	17	19	23	29
a^{-1}	1	13	11	7	23	19	17	29



```
n = 30
for a in range(n):
  if math.gcd(a, n) == 1:
    for i in range(n):
        if (a * i) % n == 1:
          a_inv = i
          print(f"a = {a}, a^-1 = {a_inv}")
          break
```

```
a = 1, a^-1 = 1
a = 7, a^-1 = 13
a = 11, a^-1 = 11
a = 13, a^-1 = 7
a = 17, a^-1 = 23
a = 19, a^-1 = 19
a = 23, a^-1 = 17
a = 29, a^-1 = 29
```

c) a=37, b=58

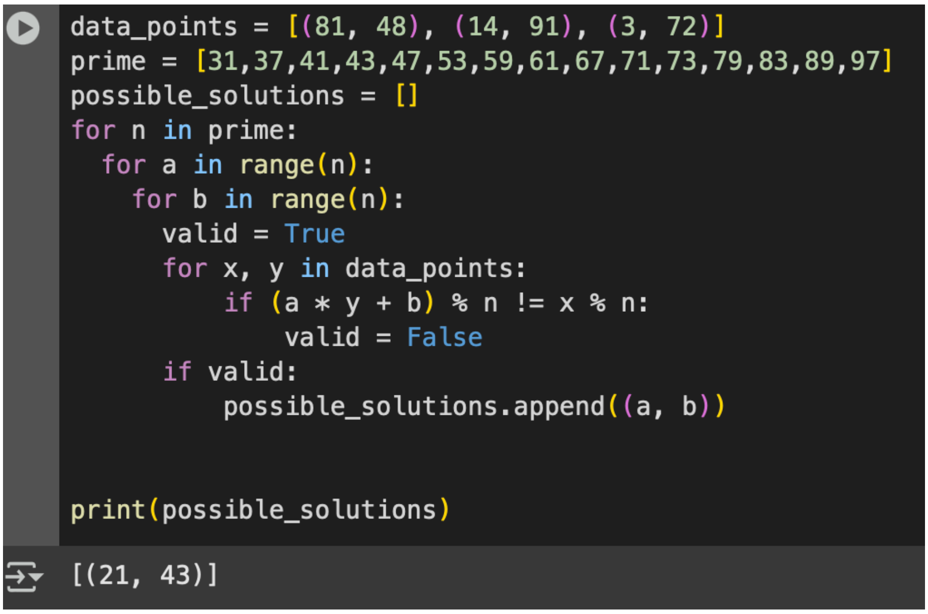


```
data_points = [(81, 48), (14, 91), (3, 72)]
prime = [31,37,41,43,47,53,59,61,67,71,73,79,83,89,97]
possible_solutions = []
for n in prime:
  for a in range(n):
    for b in range(n):
      valid = True
      for x, y in data_points:
          if (a * x + b) % n != y % n:
              valid = False
      if valid:
          possible_solutions.append((a, b))


print(possible_solutions)
```

```
[(37, 58)]
```

d) c=21, d=43

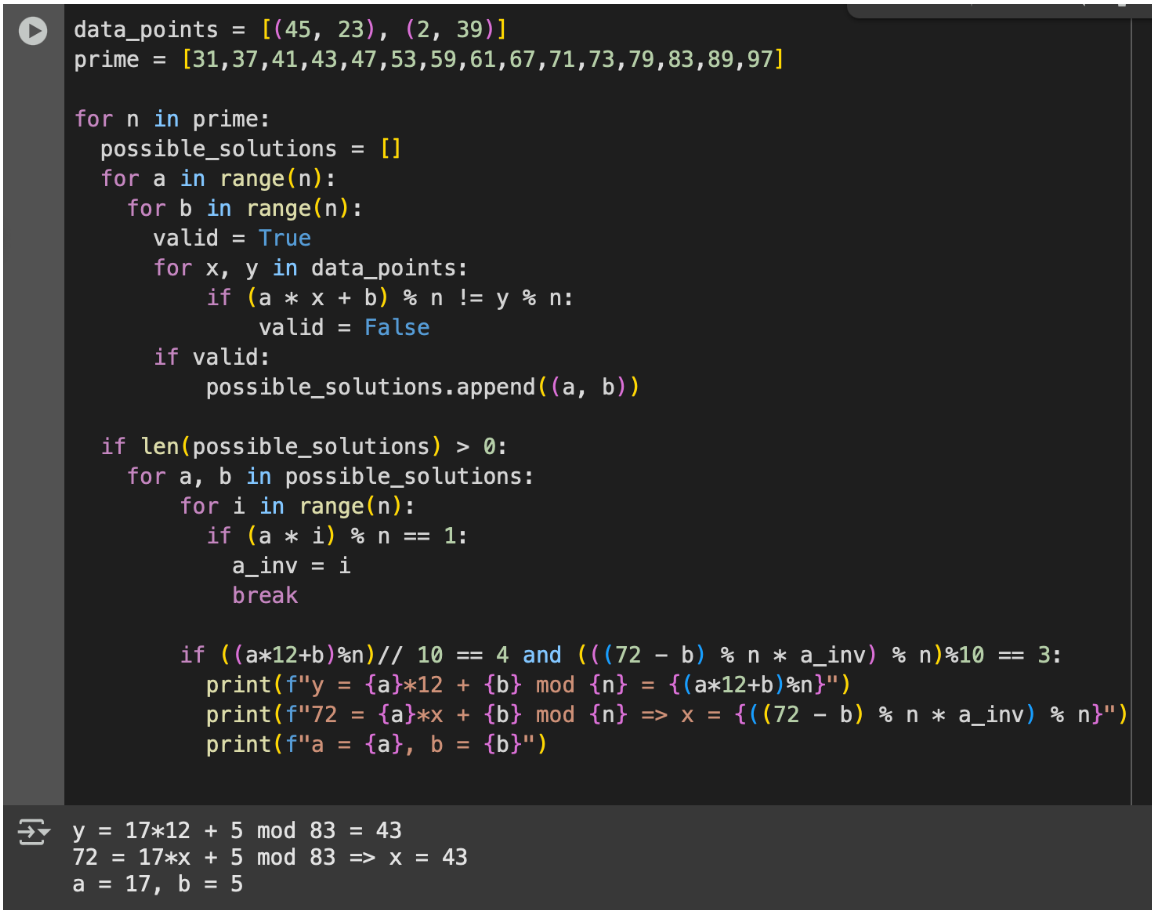


```
data_points = [(81, 48), (14, 91), (3, 72)]
prime = [31,37,41,43,47,53,59,61,67,71,73,79,83,89,97]
possible_solutions = []
for n in prime:
  for a in range(n):
    for b in range(n):
      valid = True
      for x, y in data_points:
          if (a * y + b) % n != x % n:
              valid = False
      if valid:
          possible_solutions.append((a, b))


print(possible_solutions)
```

```
[(21, 43)]
```

e) a = 17, b = 5



```
data_points = [(45, 23), (2, 39)]
prime = [31,37,41,43,47,53,59,61,67,71,73,79,83,89,97]

for n in prime:
  possible_solutions = []
  for a in range(n):
    for b in range(n):
      valid = True
      for x, y in data_points:
          if (a * x + b) % n != y % n:
              valid = False
      if valid:
          possible_solutions.append((a, b))

  if len(possible_solutions) > 0:
    for a, b in possible_solutions:
        for i in range(n):
          if (a * i) % n == 1:
            a_inv = i
            break

        if ((a*12+b)%n)// 10 == 4 and (((72 - b) % n * a_inv) % n)%10 == 3:
          print(f"y = {a}*12 + {b} mod {n} = {(a*12+b)%n}")
          print(f"72 = {a}*x + {b} mod {n} => x = {((72 - b) % n * a_inv) % n}")
          print(f"a = {a}, b = {b}")
```

```
y = 17*12 + 5 mod 83 = 43
72 = 17*x + 5 mod 83 => x = 43
a = 17, b = 5
```