a) Prebrojavanjem lako utvrđujemo da se u šifrovanoj poruci najviše puta pojavljuje slovo W (19 puta), a zatim slovo Y (8 puta). Stoga je razumno pretpostaviti da je šifriranje dovelo do zamjene slova A slovom W, i slova E slovom Y. Kako slova A, W, E i Y imaju redom ASCII šifre 65, 87, 69 i 89, to uz navedenu pretpostavku a i b moraju zadovoljavati sljedeći sistem jednačina

$$\mathrm{mod}(65\,a + b, 26) + 65 = 87$$
$$\mathrm{mod}(69\,a + b, 26) + 65 = 89$$

odnosno sistem

$$\mathrm{mod}(65\,a + b, 26) = 22$$
$$\mathrm{mod}(69\,a + b, 26) = 24$$

Ove jednačine možemo zapisati kao sljedeće kongruencije

$$65\,a + b \equiv 22 \pmod{26}$$
$$69\,a + b \equiv 24 \pmod{26}$$

Oduzimanjem prve kongruencije od druge dobijamo linearnu kongruenciju $4\,a \equiv 2 \pmod{26}$, čije je tipično rješenje tražena vrijednost za a. Ova kongruencija se svodi na linearnu Diofantovu jednačinu $4\,a + 26\,k = 2$. Kako je $\mathrm{NZD}(4, 26) = 2$, jednačinu treba podijeliti sa 2, čime ona postaje $2\,a + 13\,k = 1$. Primjenom proširenog Euklidovog algoritma odmah u prvom koraku dobijamo:

$$13 = 6 \cdot 2 + 1 \;\Rightarrow\; 1 = 13 - 6 \cdot 2 = -6 \cdot 2 + 1 \cdot 13$$

Stoga je opće rješenje za a dato kao $a = -6 \cdot 1 + 13\,t = -6 + 13\,t$, gdje je t proizvoljan cijeli broj. Tipična rješenje dobijamo za $t = 1$ i $t = 2$, i ona glase redom $a = 7$ i $a = 20$.

Kada smo našli moguće vrijednosti za a, moguće vrijednosti b lako nalazimo iz neke od polaznih kongruencija. Uzmimo, na primjer, kongruenciju $65\,a + b \equiv 22 \pmod{26}$. Iz nje neposredno slijedi $b \equiv 22 - 65\,a \pmod{26}$. Za Za $a = 7$ odnosno $a = 20$ dobijamo redom $b \equiv -433 \pmod{26}$ odnosno $b \equiv -1278 \pmod{26}$. To zapravo znači da je $b = -433 + 26\,t$ odnosno $b = -1278 + 26\,t$ gdje je t proizvoljan cijeli broj. Ograničenje $0 \le b \le 25$ nameće da mora biti $t = 17$ odnosno $t = 50$, što na kraju daje $b = 9$ odnosno $b = 22$.

U ovom trenutku smo došli do zaključka da postoje dva moguća rješenja za a i b koja dovode do toga da se A preslikava u W, a E u Y. Jedna mogućnost je $a = 7$ i $b = 9$, dok je druga mogućnost $a = 20$ i $b = 22$. U dijelu pod b) ćemo vidjeti da će na osnovu same strukture šifrovane poruke druga mogućnost otpasti kao nerealna. Međutim, uz malo razmišljanja možemo to zaključiti i odmah. Naime, kada bi bilo $a = 20$ i $b = 22$, funkcija šifriranja bi glasila $y = \mathrm{mod}(20\,x + 22, 26) + 65$. Kako je $20\,x + 22$ uvijek paran broj i kako je 26 također paran broj, to je i $\mathrm{mod}(20\,x + 22, 26)$ uvijek paran, odnosno y je uvijek neparan. Dakle, kada bi funkcija šifriranja zaista imala ovakav oblik, šifrirana poruka bi mogla sadržavati samo znakove sa neparnim ASCII šiframa. To međutim nije tačno, jer šifrirana poruka sadrži recimo slovo D, čija je ASCII šifra 68. Slijedi da mora biti $a = 7$ i $b = 9$. Ovaj zaključak će biti egzaktno potvrđen u dijelu pod b).

b) Sada znamo da funkcija šifriranja tačno glasi $y = \mathrm{mod}(7\,x + 9, 26) + 65$ (kasnije ćemo, radi potpunosti, razmotriti šta bi se dogodilo ukoliko bismo pretpostavili da funkcija šifriranja glasi $y = \mathrm{mod}(20\,x + 22, 26) + 65$). Za dobijanje funkcije dešifriranja treba ovaj izraz riješiti po x, uz dodatni uvjet $65 \le x < 91$. Radi lakšeg rada, uzmimo smjenu $x = 65 + x'$, tako da dodatni uvjet postaje $0 \le x' < 26$, odnosno, tražićemo tipično rješenje za x'. Izrazimo funkciju šifriranja preko x' umjesto preko x:

$$y = \mathrm{mod}(7x + 9, 26) + 65 = \mathrm{mod}(7(65 + x') + 9, 26) + 65 =$$
$$= \mathrm{mod}(7x' + 464, 26) + 65 = \mathrm{mod}(7x' + 22, 26) + 65$$

Ovu formulu možemo zapisati u obliku $y - 65 = \mathrm{mod}(7x' + 22, 26)$ odnosno kao kongruenciju $y - 65 \equiv 7x' + 22 \pmod{26}$, koja se dalje svodi na kongruenciju $7x' \equiv y - 87 \pmod{26}$. U ovoj kongruenciji x' treba posmatrati kao nepoznatu, a y kao parametar. Ova kongruencija dalje vodi ka Diofantovoj jednačini $7x' + 26k = y - 87$ u kojoj je y također parametar. Kako je NZD(7, 26) = 1, ova jednačina je rješiva za svaku vrijednost y, te odmah možemo primjeniti prošireni Euklidov algoritam:

$$26 = 3 \cdot 7 + 5 \;\Rightarrow\; 5 = 26 - 3 \cdot 7$$
$$7 = 1 \cdot 5 + 2 \;\Rightarrow\; 2 = 7 - 5 = 7 - (26 - 3 \cdot 7) = 4 \cdot 7 - 26$$
$$5 = 2 \cdot 2 + 1 \;\Rightarrow\; 1 = 5 - 2 \cdot 2 = (26 - 3 \cdot 7) - 2 \cdot (4 \cdot 7 - 26) = -11 \cdot 7 + 3 \cdot 26$$

Odavde je opće rješenje za x' dato kao $x' = -11 \cdot (y - 87) + 26t = 957 - 11y + 26t$ gdje je t ma kakav cijeli broj. Nevolja je što bi sada t trebalo birati tako da se zadovolji uvjet $0 \le x' < 26$, a takav t može zavisiti od toga koliki je y. Mada je moguće eksplicitno izvesti takvu zavisnost, postoji jednostavniji način da se izvede izraz za x' kod kojeg je taj uvjet automatski ispunjen. Naime, izraz $x' = 957 - 11y + 26t$, $t \in \mathbb{Z}$ proizvoljno može se napisati u obliku kongruencije $x' \equiv 957 - 11y \pmod{26}$ odnosno $x' \equiv 21 - 11y \pmod{26}$ nakon izvršene redukcije koeficijenata po modulu 26. Ako sad stavimo $x' = \mathrm{mod}(21 - 11y, 26)$, biće zadovoljena i kongruencija i dodatni uvjet $0 \le x' < 26$. Ovim smo našli formulu za određivanje x'. Mada je ova formula korektna, moguće joj je dati neznatno ljepši oblik, s obzirom da će pomoću ove formule izraz $21 - 11y$ uvijek biti negativan. Kako očigledno vrijedi $\mathrm{mod}(p, q) = \mathrm{mod}(p + kq, q)$ za ma kakav cijeli broj k, moguće je u formuli za x' dodati $26y$ na izraz $21 - 11y$ a da se vrijednost za x' ne promijeni, čime dolazimo do praktičnije ekvivalentne formule $x' = \mathrm{mod}(15y + 21, 26)$. Konačno, s obzirom da je $x = 65 + x'$, funkcija dešifriranja glasi $x = \mathrm{mod}(15y + 21, 26) + 65$.

Demonstrirajmo još jedan alternativni način da se izvede ista formula, koji je možda čak i praktičniji. Naime, kongruenciju $7x' \equiv y - 87 \pmod{26}$ možemo drugačije zapisati i kao jednačinu u modularnoj aritmetici $[7x']_{26} = [y - 87]_{26}$, odnosno kao $[7]_{26} \cdot [x']_{26} = [y - 87]_{26}$. Pomnožimo li obje strane pretodne jednačine sa $([7]_{26})^{-1}$, direktno dobijamo $[x']_{26} = ([7]_{26})^{-1} \cdot [y - 87]_{26}$, jer je $([7]_{26})^{-1} \cdot [7]_{26} = [1]_{26}$. Sada samo treba naći $([7]_{26})^{-1}$. Označimo li $([7]_{26})^{-1} = [u]_{26}$, znamo da se u može dobiti rješavanjem Diofantove jednačine $7u + 26k = 1$. Kako smo rastavu $1 = -11 \cdot 7 + 3 \cdot 26$ već našli ranije, odmah možemo pisati $u = -11 \cdot 1 + 26t = -11 + 26t$ gdje je t proizvoljan cijeli broj, odnosno $u = 15$ ako tražimo tipično rješenje (koje slijedi za $t = 1$). Dakle, imamo

$$[x']_{26} = ([7]_{26})^{-1} \cdot [y - 87]_{26} = [15]_{26} \cdot [y - 87]_{26} = [15y - 1305]_{26} = [15y - 5]_{26}$$

s obzirom da je $\mathrm{mod}(1305, 26) = 5$. Stoga je $x' = \mathrm{mod}(15y - 5, 26)$. Alternativno, mogli smo dobiti i ekvivalentni oblik $x' = \mathrm{mod}(15y + 21, 26)$, jer je $[-5]_{26} = [21]_{26}$. Konačno, s obzirom da je $x = 65 + x'$, funkcija dešifriranja glasi $x = \mathrm{mod}(15y - 5, 26) + 65$. Vidimo da smo dobili isto rješenje kao i na prvi način.

Da bi se uvjerili da je ovo zaista jedino rješenje, odnosno da pretpostavka $a = 20$ i $b = 22$ nije održiva, provedimo sada isti postupak uz pretpostavku da je $a = 20$ i $b = 22$, odnosno da funkcija šifriranja glasi $y = \mathrm{mod}(20x + 22, 26) + 65$). Ponovo ćemo uvesti smjenu $x = 65 + x'$, i izraziti ovu funkciju preko x' umjesto preko x:

$$y = \mathrm{mod}(20x + 22, 26) + 65 = \mathrm{mod}(20(65 + x') + 22, 26) + 65 =$$
$$= \mathrm{mod}(20x' + 1332, 26) + 65 = \mathrm{mod}(20x' + 6, 26) + 65$$

Slično kao u prvom slučaju, ovu formulu možemo zapisati u obliku $y-65 = \mathrm{mod}(20x' + 6, 26)$ odnosno kao kongruenciju $y-65 \equiv 20x' + 6 \pmod{26}$, koja se dalje svodi na kongruenciju $20x' \equiv y-71 \pmod{26}$. Ova kongruencija vodi ka Diofantovoj jednačini $20x' + 26k = y-87$ u kojoj je y parametar. Kako je $\mathrm{NZD}(20, 26) = 2$, ova jednačina ima rješenje po x' samo ukoliko je $2 \mid y-71$, što je ispunjeno samo ako je $y-71$ paran, odnosno ako je y neparan. Dakle, rješenje za x' (pa samim tim i za x) postoji samo za neparne vrijednosti y. Odavde slijedi da ne postoji inverzna funkcija koja bi davala vrijednosti x za proizvoljne vrijednosti y uz ovakvu funkciju šifriranja, što automatski isključuje mogućnost da je bila primijenjena takva funkcija šifriranja, s obzirom da šifrirana poruka sadrži i parne vrijednosti za y. Treba još primijetiti da alternativni metod množenja sa inverznim elementom u ovom slučaju nije direktno primjenljiv. Naime, mada se kongruencija $20x' \equiv y-71 \pmod{26}$ može zapisati u obliku $[20]_{26} \cdot [x']_{26} = [y-71]_{26}$, ovdje nije moguće prosto pomnožiti obje strane ove jednačine sa $([20]_{26})^{-1}$, s obzirom da $([20]_{26})^{-1}$ ne postoji, jer je $\mathrm{NZD}(20, 26) \neq 1$.

c) Sad kada znamo da funkcija za dešifriranje glasi $x = \mathrm{mod}(15y + 21, 26) + 65$, nije teško sastaviti tablicu koja daje vrijednosti x za sve moguće vrijednosti y od 65 do 90 uključivo. Izračunavanje daje sljedeću tablicu:

y	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
x	73	88	77	66	81	70	85	74	89	78	67	82	71	86	75	90	79	68	83	72	87	76	65	80	69	84

Alternativno, izraženo preko ASCII kôdova, ova tablica izgleda ovako:

y	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
x	I	X	M	B	Q	F	U	J	Y	N	C	R	G	V	K	Z	O	D	S	H	W	L	A	P	E	T

Sada, zamjena svakog znaka u primljenom tekstu odgovarajućim znakom iz ove tablice daje sljedeći dešifrirani tekst:

NAJBOLJINACINDASESAVLADADISKRETNAMATEMATIKAJEKROZRJESAVANJEVE
CEGBROJADOBROODABRANIHZADATAKA

Odnosno, uz dodavanje malo razmaka za poboljšanje čitljivosti:

NAJBOLJI NACIN DA SE SAVLADA DISKRETNA MATEMATIKA JE KROZ
RJESAVANJE VECEG BROJA DOBRO ODABRANIH ZADATAKA