Tworzenie klucza:

$p = 97$

$q = 211$

$n = p \cdot q = 97 \cdot 211 = 20467$

$\varphi = (p-1)(q-1) = 96 \cdot 210 = 20160$

za e bierzemy liczbę np. 17 i sprawdzamy za pomocą algorytmu Euklidesa czy e i φ są względnie pierwsze

krok	a	b
1	20160	17
2	17	15
3	15	2
4	2	1
5	1	0

$NWD(17, 20160) = 1$

zatem e może być równe 17

Teraz musimy znaleźć d, spełniające równanie: $\varphi \bmod (e \cdot d) = 1$

do tego posłużymy rozszerzony algorytm Euklidesa:

$\varphi \cdot y + e \cdot x = 1$

krok	a	q	s	t
0	20160		1	0
1	17	1185	0	1
2	15	1	1	-1185
3	2	7	-1	1186
4	1	2	8	-9487
5	0		-9	10673

Sprawdzamy:

$-9 \cdot 20160 + 10673 \cdot 17 = 1$

$1 = 1$

$L = P$

zatem: $d = 10673$

klucz publiczny

$(e, n) = (17, 20467)$

klucz tajny

$(d, n) = (10673, 20467)$

Szyfrowanie:

$s = t^e \bmod n$

Litera	t	s
M	17	14440
A	1	1
T	26	1515
E	7	5393
U	27	2840
S	24	10291
Z	30	6178

Zaszyfrowana wiadomość:

14440-1-1515-5393-2840-10291-6178

Deszyfrowanie:

$t = s^d \bmod n$

$14440^{10673} \bmod 20467 = 17 \Rightarrow M$

$1^{10673} \bmod 20467 = 1 \Rightarrow A$

$1515^{10673} \bmod 20467 = 26 \Rightarrow T$

$5393^{10673} \bmod 20467 = 7 \Rightarrow E$

$2840^{10673} \bmod 20467 = 27 \Rightarrow U$

$10291^{10673} \bmod 20467 = 24 \Rightarrow S$

$6178^{10673} \bmod 20467 = 30 \Rightarrow Z$