W oryginalnej definicji szyfrów podstawieniowych zakładano, że w tekście jawnym nie ma spacji ani znaków przestankowych, nie rozróżniano też małych i wielkich liter. Zmniejszało to bardzo czytelność tekstów, od tych założeń odchodzimy. Pewnym problemem jest też obecność polskich liter, można tekst jawny poddać wstępnemu przetwarzaniu i założyć, że polskie litery zostały usunięte, można też przyjąć, że alfabet jest dłuższy niż w języku angielskim i zmodyfikować odpowiednio algorytmy.

Zakładamy, że litery zakodowane są za pomocą liczb 0..25, spacje, znaki przestankowe i cyfry pozostaną nienaruszone, niezmieniona też będzie wielkość liter (tzn. małe litery będziemy szyfrować za pomocą małych liter, a wielkie wielkimi literami. Zmniejsza to oczywiście radykalnie bezpieczeństwo szyfru, ale jest ono i tak bliskie zeru.

W poniższym x oznacza tekst jawny, y kryptogram, k klucz, E funkcję szyfrującą, a D funkcję odszyfrowywania.

- szyfr Cezara: $E(k,x)=x+k \pmod{26}$, $D(k,y)=y-k \pmod{26}$, klucz k jest liczbą z zakresu 1..25.
- szyfr afiniczny: $E(a,b,x)=a*x+b \pmod{26}$, $D(a,b,y)=a'*(y-b) \pmod{26}$ gdzie klucz jest parą liczb (a,b) takich, że NWD(a,26)=1 oraz $a*a'=1 \pmod{26}$.