Polyal-
pha-
betic
Ci-
pher
polyal-
pha-
betic
ci-
pher
monoal-
pha-
betic
ci-
pher
??
$_0, c_1, c_2, ..., c_{n-1}$
$_0, k_1, ..., k_{m-1})(p_0, p_1, ..., p_{n-1})]$
$_0+$
$k_0)mod26, (p_1+$
$k_1)mod26, ..., (p_{m-1}+$
$k_{m-1})mod26,$
$_m+$
$k_0)mod26, (p_{m+1}+$
$k_1)mod26, ..., (p_{2m-1}+$
$k_{m-1})mod26, ...$
Polyal-
pha-
bet-
i-
cal
Ci-
pher
polyal-
pha-
betic
ci-
pher
Vi-
genere
Ci-
pher
?
Ci-
pher-
text
polyal-
pha-
bet-
i-
cal
ci-
pher
?
Plain-
text
?
Se-
cret
Key
key
?
polyal-
pha-
bet-
i-
cal
ci-
pher
Ka-
siski
Ex-
am-
i-
na-
tion
ci-
pher-
text
polyal-
pha-
bet-
i-
cal
ci-
pher
monoal-
pha-
bet-
i-
cal
ci-
pher
sub-
tring
sub-
tring
??
ciphertext