$f_E :$
$P \rightarrow$
C
P
C
f_E
$f_E^{-1} \equiv$
f_D
D
A
D
B
E
C
F
$f(x) =$
$x+$
$3 mod 26$
$f^{-1}(x) =$
$x-$
$3 mod 26$
$f_b(x) =$
$x+$
$b mod 26, f_b^{-1}(x) =$
$x+$
$(-b) mod 26$
b
D
E
$f_E(x)$
D
E
D
(i)
d_i
e_i
d_i
e_i
e_A
d_A
d_A
e_B
d_B
$f(x) =$
$g^x p$
p
Z_p
$g \in$
Z_p
$\alpha \in$
$\{2, \ldots, p-$
$1\}$
$g^\alpha p$
$\beta \in$
$\{2, \ldots, p-$
$1\}$
$g^\beta p$
$k_\alpha =$
$\left(g^\beta\right)^\alpha p$
$k_\beta =$
$(g^\alpha)^\beta p$
$k =$
$k_\alpha =$
k_β
f
$P \neq$
NP
$\mathbf{?}$
G
$g, x \in$
G
$x =$
$x^{-1} g x$
g
x
G
$g, h \in$
G
$h_x =$
g^x
$x \in$
G
g
h
$y \in$
G
$h_y =$
g^y
g, h
y
$h =$
$y^{-1} g y$
$\mathbf{?}$
G
$g \in$
G