❍❛ ✈❛ ❞ ❯♥✐✈❡ ✐ ② ❙❛❧✐❧ ❱❛❞❤❛♥

# ❈❙ ✶✷✼✿ ■♥ ♦❞✉❝ ✐♦♥ ♦ ❈ ②♣ ♦❣ ❛♣❤②

◗✉✐③ ■ ❛❝ ✐❝❡ ♦❜❧❡♠

❙❡♣ ❡♠❜❡ ✷✾✱ ✷✵✶✸

❏✉ ✐❢② ❛❧❧ ♦❢ ②♦✉ ❛♥ ✇❡ ✳ ❚❤✐ ❛❧ ♦ ❛♣♣❧✐❡ ♦ ✉❡ ✐♦♥ ✇❤✐❝❤ ❛ ❡ ♥♦ ♣✉ ❡❧② ♠❛ ❤❡♠❛ ✐❝❛❧✱

❢♦ ✇❤✐❝❤ ②♦✉ ❤♦✉❧❞ ❜❛❝❦ ✉♣ ②♦✉ ❛♥ ✇❡ ✇✐ ❤ ♠❛ ❤❡♠❛ ✐❝❛❧ ❡①♣❧❛♥❛ ✐♦♥ ✳ ❨♦✉ ♠❛② ❛ ✉♠❡ ❛❧❧

❡ ✉❧ ♣ ♦✈❡♥ ✭♦ ❛ ❡❞ ❛ ❛ ❢❛❝ ✮ ✐♥ ❝❧❛ ♦ ♦♥ ❤❡ ♣ ♦❜❧❡♠ ❡ ✳ ❚❤✐ ❡ ♦❢ ♣ ❛❝ ✐❝❡ ♣ ♦❜❧❡♠ ✐

♦✉❣❤❧② ✇✐❝❡ ❤❡ ❧❡♥❣ ❤ ♦❢ ❤❡ ❛❝ ✉❛❧ ✉✐③✳

h ♦❜❧❡♠ ✶✳

✶✳ ❙ ❛ ❡ ❤❡ ❞❡✜♥✐ ✐♦♥ ♦❢ ❤❡ ♦♥❡✲ ✐♠❡ ♣❛❞ ❡♥❝ ②♣ ✐♦♥ ❝❤❡♠❡ ❢♦ *n*✲❜✐ ♠❡ ❛❣❡ ✳ ❨♦✉ ♣❡❝✐✜✲

❝❛ ✐♦♥ ❤♦✉❧❞ ✐♥❝❧✉❞❡✿ ❤❡ ♠❡ ❛❣❡ ♣❛❝❡✱ ❤❡ ❝✐♣❤❡ ❡① ♣❛❝❡✱ ❤❡ ❦❡② ♣❛❝❡✱ ❛♥❞ ❢✉♥❝ ✐♦♥

Gen✱ Enc*k* ❛♥❞ Dec*k* ✳

✷✳ ❲❤② ✐ ❤❡ ♦♥❡✲ ✐♠❡ ♣❛❞ ♥♦ ❝♦♠♠♦♥❧② ✉ ❡❞ ✐♥ ♣ ❛❝ ✐❝❡❄

h ♦❜❧❡♠ ✷✳ ✭❑▲ ❡①❡ ❝✐ ❡ ✷✳✻✱ ♠♦❞✐✜❡❞✮ ❲❤❡♥ ✉ ✐♥❣ ❤❡ ♦♥❡✲ ✐♠❡ ♣❛❞ ✇✐ ❤ ❤❡ ❦❡② 0*n*✱

❤❡ ❡♥ ✐ ❡ ♠❡ ❛❣❡ ✐ ❡♥ ✐♥ ❤❡ ❝❧❡❛ ✳ ■ ❤❛ ❤❡ ❡❢♦ ❡ ❜❡❡♥ ✉❣❣❡ ❡❞ ❤❛ ❤❡ ♦♥❡✲ ✐♠❡ ♣❛❞

❜❡ ♠♦❞✐✜❡❞ ❜② ♦♥❧② ❡♥❝ ②♣ ✐♥❣ ✇✐ ❤ ❦❡② *k* =

0*n* ❝❤♦ ❡♥ ✉♥✐❢♦ ♠❧② ❛ ❛♥❞♦♠✳ ■ ❤❡ ❡ ✉❧ ✐♥❣

❝❤❡♠❡ ✐❧❧ ♣❡ ❢❡❝ ❧② ❡❝ ❡ ❄ ❲❤❛ ✐ ❤❡ ♠❛❧❧❡ *ε ≥* 0 ❢♦ ✇❤✐❝❤ ❤✐ ❝❤❡♠❡ ❤❛ ❛ ✐ ✐❝❛❧❧②

*ε*✲✐♥❞✐ ✐♥❣✉✐ ❤❛❜❧❡ ❡♥❝ ②♣ ✐♦♥ ❄ ❲♦✉❧❞ ✇❡ ✇❛♥ ♦ ♠❛❦❡ ✉❝❤ ❛ ♠♦❞✐✜❝❛ ✐♦♥ ✐♥ ♣ ❛❝ ✐❝❡❄

h ♦❜❧❡♠ ✸✳ ❋♦ ❡❛❝❤ ♦❢ ❤❡ ❢♦❧❧♦✇✐♥❣✱ ❛♥ ✇❡ ✇❤❡ ❤❡ ✐ ✐ ❚❘❯❊ ♦ ❋❆▲❙❊ ❢♦ ❡❛❝❤ ♦❢ ❤❡

♥♦ ✐♦♥ ♦❢ ♣❡ ❢❡❝ ❡❝ ❡❝②✱ ❛ ✐ ✐❝❛❧ ❡❝✉ ✐ ②✱ ❛♥❞ ❝♦♠♣✉ ❛ ✐♦♥❛❧ ❡❝✉ ✐ ②✳

✶✳ ❆ ✉♠❡ ❛♥ ❛❞✈❡ ❛ ② ✇✐ ❤ ❧✐♠✐ ❡❞ ❝♦♠♣✉ ❛ ✐♦♥ ✐♠❡

✷✳ ♦✈✐❞❡ ♣ ✐✈❛❝② ❢♦ ❡❛❝❤ ✐♥❞✐✈✐❞✉❛❧ ❜✐ ♦❢ ❛ ♠❡ ❛❣❡

✸✳ ▼❛② ❛❧❧♦✇ ❛♥ ❛❞✈❡ ❛ ② ♦ ✏❜ ❡❛❦✑ ❤❡ ❝❤❡♠❡ ✇✐ ❤ ♦♠❡ ♠❛❧❧ ♣ ♦❜❛❜✐❧✐ ②

✹✳ ■ ❛❝❤✐❡✈❛❜❧❡ ❛ ✉♠✐♥❣ **P** = **NP**

h ♦❜❧❡♠ ✹✳ ❊❛❝❤ ❞❛②✱ ❛ ❛ ❡❧❧✐ ❡ ❡♥❞ ❛ ✐♥❣❧❡ ❡♥❝ ②♣ ❡❞ ♠❡ ❛❣❡ ❜❛❝❦ ♦ ❊❛ ❤ ✉ ✐♥❣ ❛ ✶✷✽✲

❜✐ ♦♥❡✲ ✐♠❡ ♣❛❞✱ ✇✐ ❤ ❛ ❢ ❡ ❤ ❦❡② ❢♦ ❡❛❝❤ ❞❛②✳ ❊❛❝❤ ♠❡ ❛❣❡ ❝♦♥ ✐ ♦❢ ❛ ✻✹✲❜✐ ✐♠❡ ❛♠♣

✭ ❤❡ ♥✉♠❜❡ ♦❢ ❡❝♦♥❞ ✐♥❝❡ ✶✾✼✵ ✐♥ ❜✐♥❛ ②✮ ❛♥❞ ❛ ✻✹✲❜✐ ♣❛②❧♦❛❞ ✭ ❤❡ ❛ ❡❧❧✐ ❡✬ ❝✉ ❡♥ ❡♥ ♦

❡❛❞✐♥❣ ✮✳ ❆ ❤❛❝❦❡ ❝❧❛✐♠ ❤❛ ✱ ❜② ❧✐ ❡♥✐♥❣ ✐♥ ♦♥ ❤❡ ❝♦♠♠✉♥✐❝❛ ✐♦♥✱ ❤❡ ✐ ❛❜❧❡ ♦ ❞❡ ❡ ♠✐♥❡ ✶✵

❜✐ ♦❢ ❤❡ ❣✐✈❡♥ ❞❛②✬ ✶✷✽✲❜✐ ♠❡ ❛❣❡✳ ■ ❤❡ ❤❛❝❦❡ ✬ ❝❧❛✐♠ ♣❧❛✉ ✐❜❧❡❄ ❉♦❡ ❤❡ ❝❤❡♠❡ ❛ ✐ ❢②

♦✉ ❞❡✜♥✐ ✐♦♥ ♦❢ ♣❡ ❢❡❝ ❡❝ ❡❝②❄

h ♦❜❧❡♠ ✺✳ ✭❑▲ ❡①❡ ❝✐ ❡ ✸✳✼✮ ❙❤♦✇ ❤❛ ✐❢ *G* ✐ ♥♦ ❛ ♣ ❡✉❞♦ ❛♥❞♦♠ ❣❡♥❡ ❛ ♦ ✱ ❤❡♥ Enc*k* (*m*) =

*G*(*k*) *⊕ m* ❞♦❡ ♥♦ ❤❛✈❡ ✐♥❞✐ ✐♥❣✉✐ ❤❛❜❧❡ ❡♥❝ ②♣ ✐♦♥ ✳

h ♦❜❧❡♠ ✻✳

✶✳ ●✐✈❡ ❤❡ ❞❡✜♥✐ ✐♦♥ ♦❢ ❛ ♣ ❡✉❞♦ ❛♥❞♦♠ ❣❡♥❡ ❛ ♦ ✳

✷✳ ❙✉♣♣♦ ❡ *G* : *{*0*,* 1*}∗ → {*0*,* 1*}∗* ✐ ❛ ♣ ❡✉❞♦ ❛♥❞♦♠ ❣❡♥❡ ❛ ♦ ✳ ❲❤✐❝❤ ♦❢ ❤❡ ❢♦❧❧♦✇✐♥❣ *Gt* ✐

♥❡❝❡ ❛ ✐❧② ❛ ♣ ❡✉❞♦ ❛♥❞♦♠ ❣❡♥❡ ❛ ♦ ❢♦ ❡✈❡ ② ♣ ❡✉❞♦ ❛♥❞♦♠ ❣❡♥❡ ❛ ♦ *G*❄ ❏✉ ✐❢② ②♦✉

❛♥ ✇❡ ✭❡✳❣✳✱ ❜② ❛ ❡❞✉❝✐❜✐❧✐ ② ❛ ❣✉♠❡♥ ♦ ❛ ❝♦✉♥ ❡ ❡①❛♠♣❧❡✮✳

✭❛✮ *Gt*(*x*) = *G*(*x*)*b*(*x*)✱ ✇❤❡ ❡ *b*(*x*) ✐ ❤❡ ❳❖❘ ♦❢ ❛❧❧ ❤❡ ❜✐ ♦❢ *G*(*x*)✳

✭❜✮ *Gt*(*x*) = *G*(*x*0*|x|*)✳

✭❝✮ *Gt*(*x*) = ❤❡ ✜ *|x|* + 1 ❜✐ ♦❢ *G*(*x*)