## 3 パスワードはなに？

あなたは，へのへのもへじ氏とパスワードを協議して決めようとしています．図 0.5 は，そのやりとりの様子を LINE 風のトーク画面にしたものです．パスワードはなんでしょう？　このやりとりで本当にパスワードは決まるのでしょうか．


**図 0.5**　パスワードを決めることはできるのか？

拙著『実験数学読本 2 [68]』の第 3.2 節でも言及しましたが，言いたいことをきちんと伝えるのはなかなか難しいものです．

さて，誰かに自分の情報やモノを渡したいとき，渡すべき人のみに渡るよ

うにするためにパスワードや暗号は必要とされています．暗号はどのように保護されているのでしょう．なんと！　まったく関係なさそうな「素因数分解は簡単にできないこと」を逆手にとって利用しています．例えば，次のような素因数分解の素朴なアルゴリズムを考えてみましょう．効率は悪いですが考え方は単純です．($A := B$ は $A$ に $B$ を代入するという意味．)

---

**Step 1**　$p := 0;\ n := N;$

**Step 2**　$n \geqq 2$ である限り以下のLoop(ループ)を続ける．

**Loop**　$m = 2, 3, \cdots, n$ に対して，以下の (1)〜(3) を続ける．

**(1)**　$j := 0;$

**(2)**　$n/m$ の余りが 0 である限り「$n := n/m;\ j := j+1;$」を繰り返す;

**(3)**　$j \geqq 1$ ならば，$m^j$ を表示して，$p := p + j;$

**Step 3**　$p \geqq 2$ ならば「$N$ は合成数」，$p = 1$ ならば「$N$ は素数」と判定．

---

**注意 0.1**　**(2)** は「割り切れる間 $n$ を $m$ で割り続けて割った回数を $j$ とする」ことに対応し，**(3)** は「$N$ は $m^j$ を因子にもつ」ことに対応している．$m$ が素数でないときは $j = 0$ となって表示されないから，$m$ は常に素数となる．また，$N$ が素数のとき $N$ 未満のいずれの $m$ でも $n = N$ を割り切ることができないからずっと $j = 0$ であるが，**Loop** 最後の $m = N$ のときのみ $n = N$ を割り切ることができて $j = 1$ となる (このとき $p = 1$)．

例えば，123456707654321(123 兆 ⋯ ) の素因数分解を，上のアルゴリズムを C 言語で書いたプログラムを著者のノートパソコンで実行してみると，$123456707654321 = 29^1 \times 41^1 \times 103832386589^1$ となります．たった 15 桁なのに数十分かかります．(一方，$29 \times 41 \times 103832386589$ の計算は一瞬です．)　もっと効率の良いアルゴリズムを作ったとしても，(実質上無理と言えるくらいに) 巨大な数の素因数分解には時間がかかります．このことを安全性の担保とした暗号方式は RSA 暗号と呼ばれ，現代の暗号秘密保全の基礎的な考え方となっています．歴史的経緯については，例えば『暗号解読 [46]』などを読むとよいでしょう．