これらの問題を速く解くアルゴリズムを探すために多大な努力がなされてきた（しかし成功していない）ことから，これらの問題は安全な暗号系を設計するために使える優良な候補であるように思えます．

残念なことに，この方針には困難があります．それで，今のところ，暗号系の設計者は（たとえば素因数分解のような）実は NP 完全問題と比べれば解くのが容易かもしれない（たぶん大幅に易しい）問題に頼らざるを得ないのです．[*11]

ここで述べたような課題に答えることは，産業界にとっては数百万ドルの価値があり，また，国防にとってはきわめて重要な問題だと考えられています．

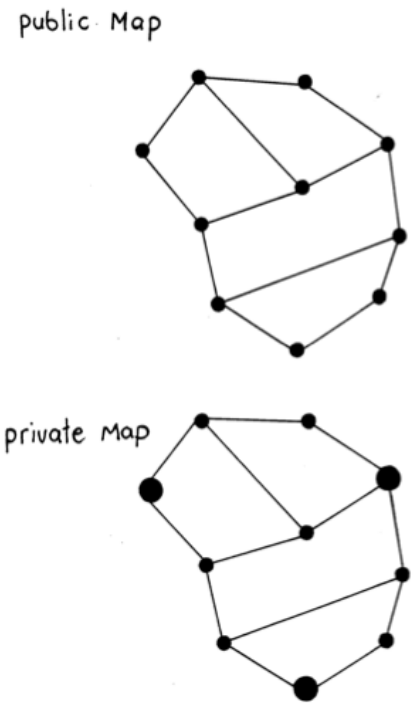
暗号理論はコンピュータサイエンスで現在非常に活発に研究されている分野です．

Further reading
参考文献

Harel の本「Algorithmics」では，公開鍵暗号系を論じています．本では，大きい素数を使って安全な公開鍵暗号系を作り出す方法を説明しています．

暗号理論についての標準的なコンピュータサイエンスの教科書は Dorothy Denning の「Cryptography and data security」です．でも，より実用的な本は Bruce Schneier の「Applied cryptography」です．

Dewdney の「Turing Omnibus」では，公開鍵暗号を実現する別の方式を説明しています．



指示：この地図を使って，本文で説明した要領で，メッセージを暗号化，復元します．

[*11] なぜ困難があるのかは明示されていませんが，NP 完全問題を使った「落とし戸つき一方向関数」が見つからないことが理由と考えられます．公開鍵暗号に使えそうな落とし戸つき一方向関数がうまく見つかるのは，えてして，NP よりずっと小さい（易しい）計算量クラスというのが（現時点での）現実のようです．