RSA暗号について

～説明文書付きヴァージョン～

※プレゼン用ではありません

RSA暗号　例をあげて説明します

２つの素数５と11を用意します

５×11＝55　を法として数を扱います。

55を法とするとは、1,2,3…53,54,0,1と
55で０に戻して数を扱うことをいいます。

55以上の数は、55で割った余りになります。

（例）55は55で割ると1あまり0で０
56は55で割ると1あまり1で１

RSA暗号

次に５と11をそれぞれ１引き
　5-1=4，11-1=10
その4と10の最小公倍数を求めると20、
それに1足して21を出します。

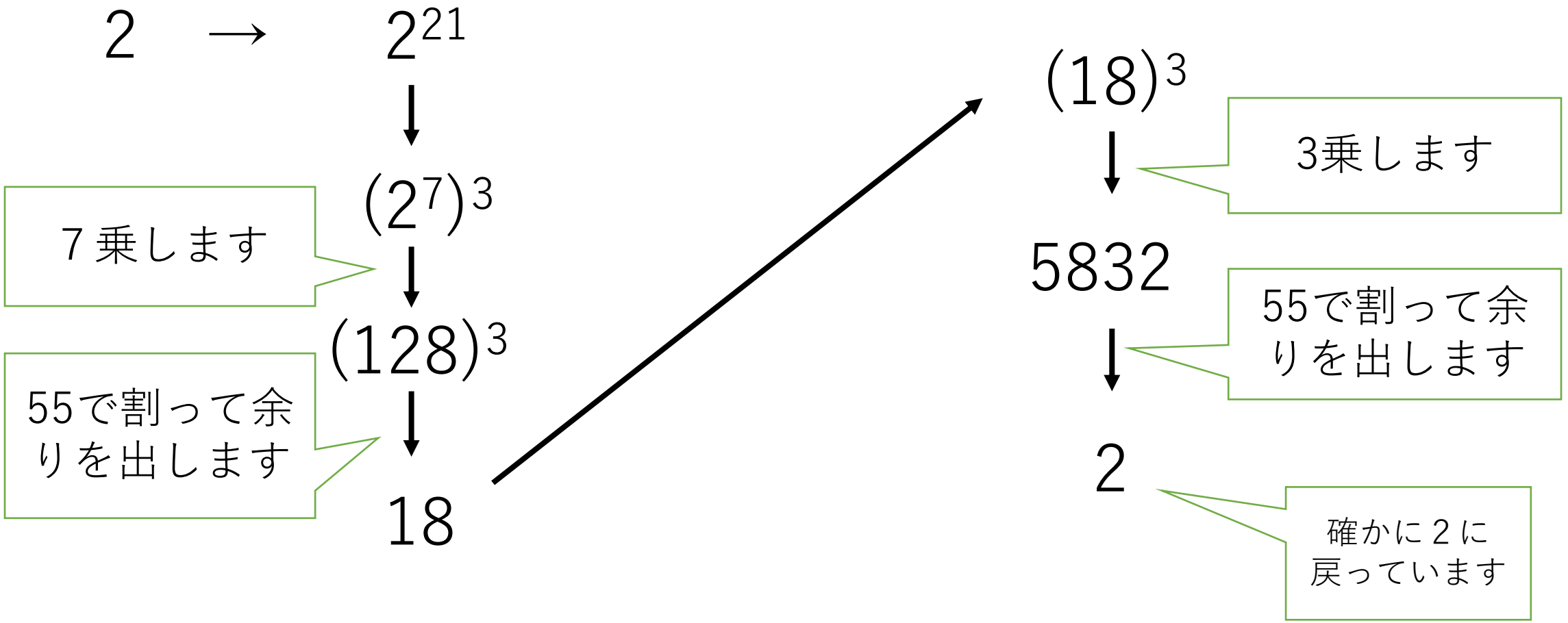
55を法として数を扱うと、
　□^{21}が□に戻る
という法則が成り立ちます。

RSA暗号

2を例に、2^{21}が2に戻るか確認します。

ここでは、$2^{21}=$を$(2^7)^3$と2回に分けて計算します。

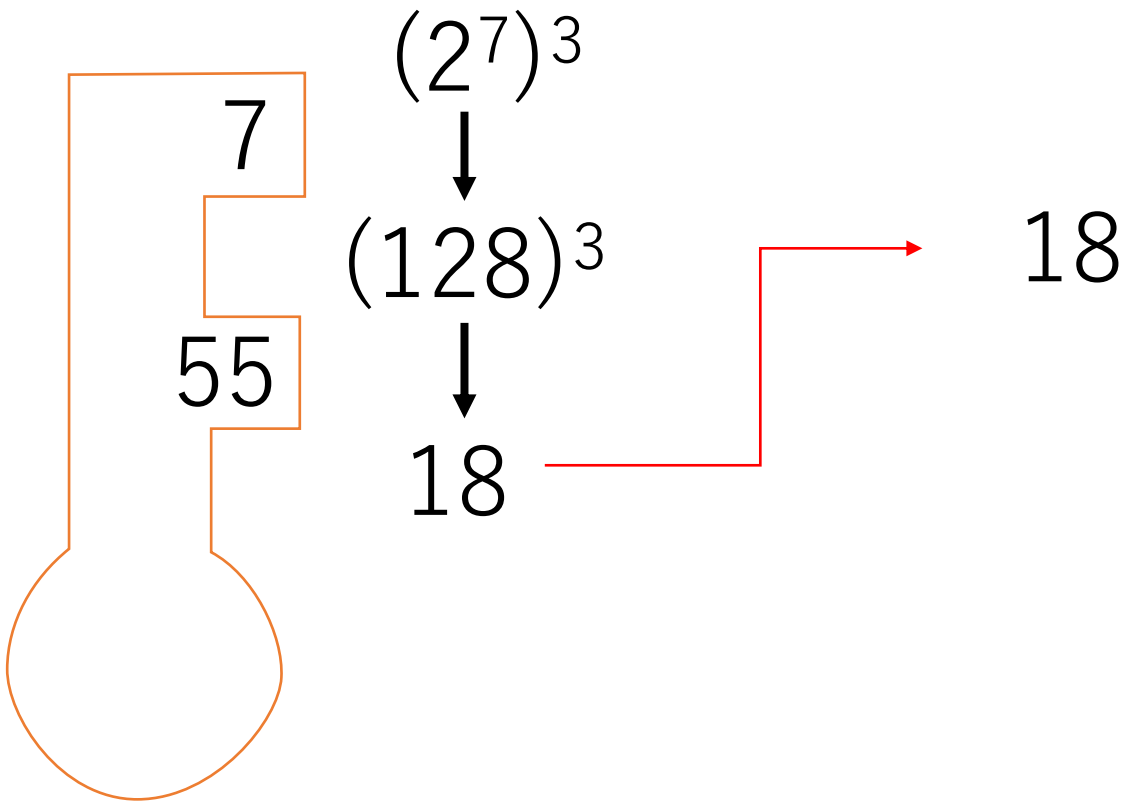
RSA暗号


2 → 2^{21}
$(2^7)^3$
$(128)^3$
18
7乗します
55で割って余りを出します
$(18)^3$
3乗します
5832
55で割って余りを出します
2
確かに2に戻っています

RSA暗号

$2 \rightarrow 2^{21}$

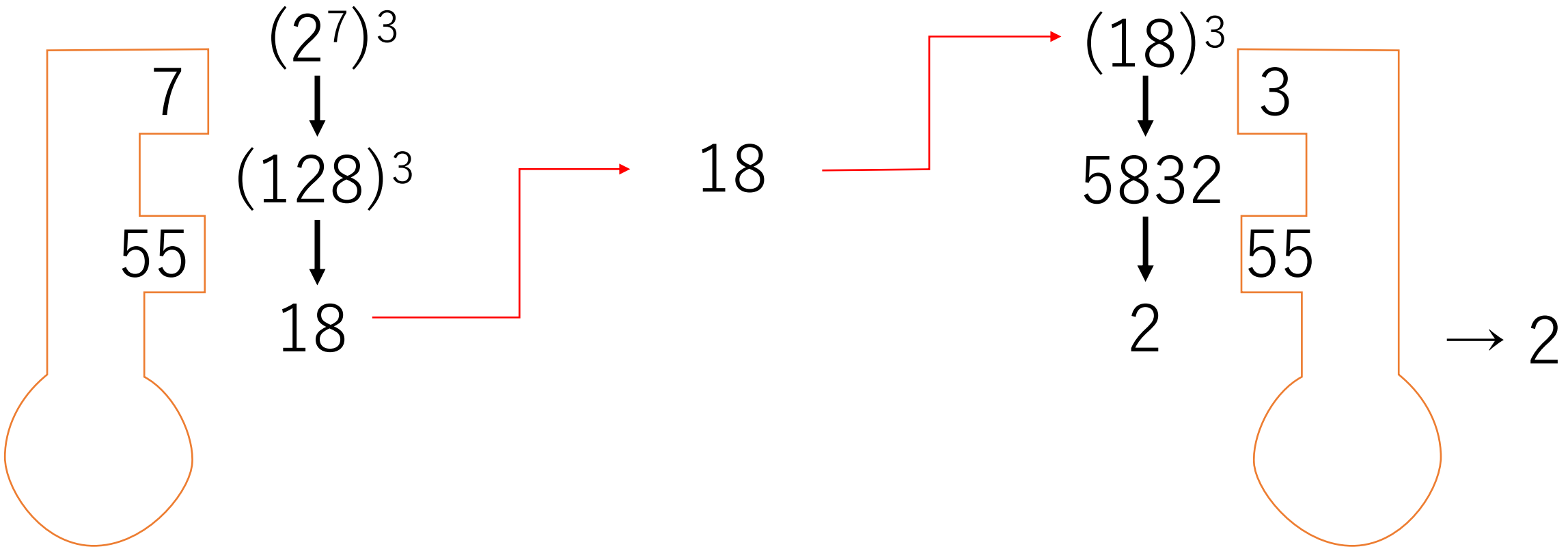
ここでかける鍵を7と55とし
出てきた18を暗号文とします



RSA暗号

$2 \rightarrow 2^{21}$

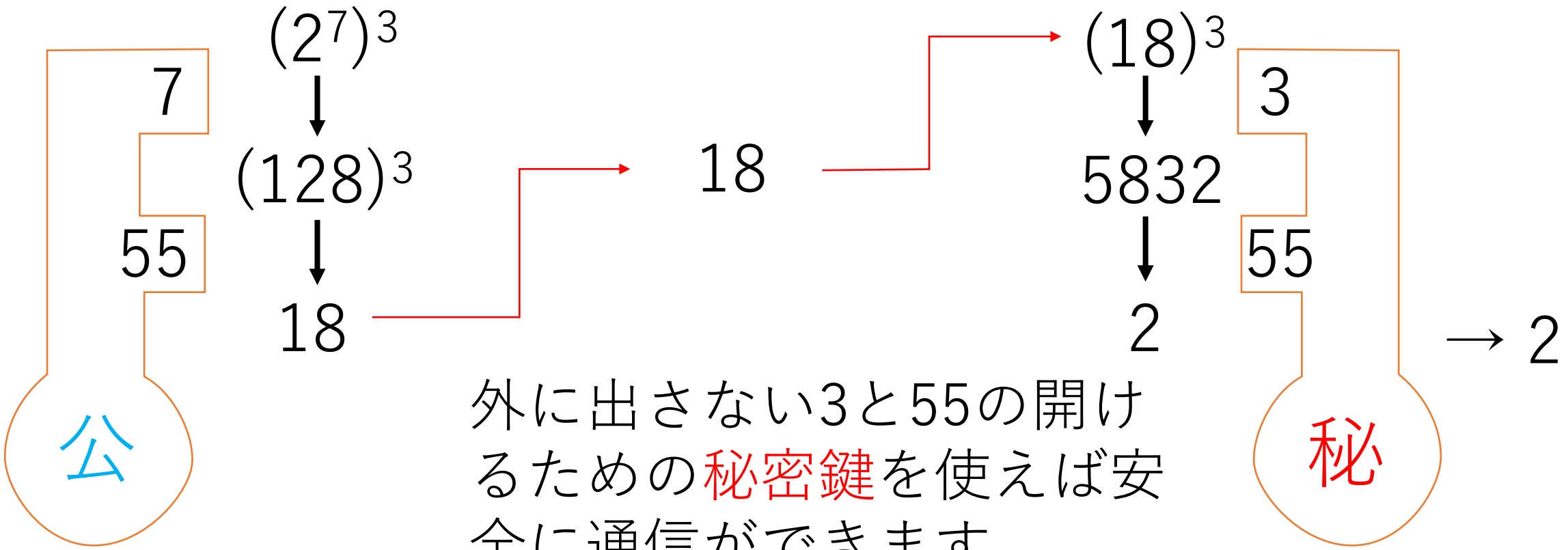
受け取った18を、開ける鍵の
3と55で2を取り出します



RSA暗号

受け取る側が7と55のかける公開鍵を渡し、

$2 \rightarrow 2^{21}$



外に出さない3と55の開けるための秘密鍵を使えば安全に通信ができます

RSA暗号

ここで、一つ気になることがあります。

公開鍵の55が5と11の積であることがわかると

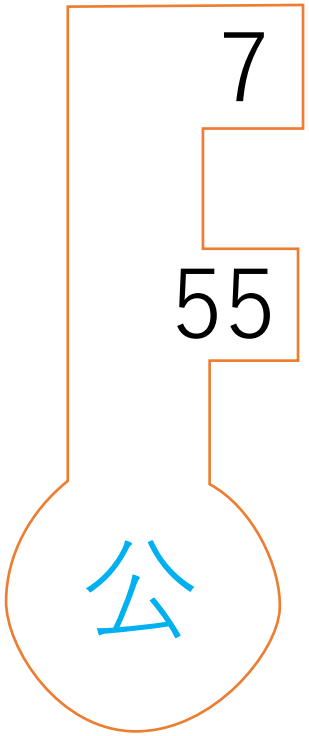
5-1=4　11-1=10

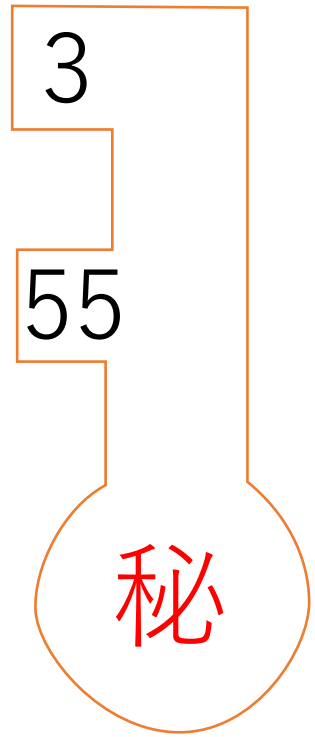
の最小公倍数を出して20

20+1＝21

21＝7×(秘密鍵の１つ)

となって、3が公開鍵から求められてしまいます。

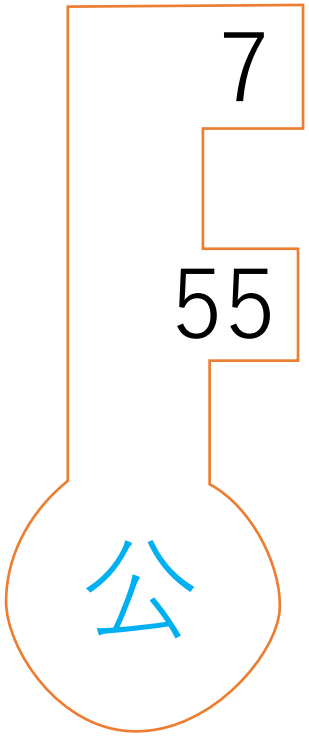


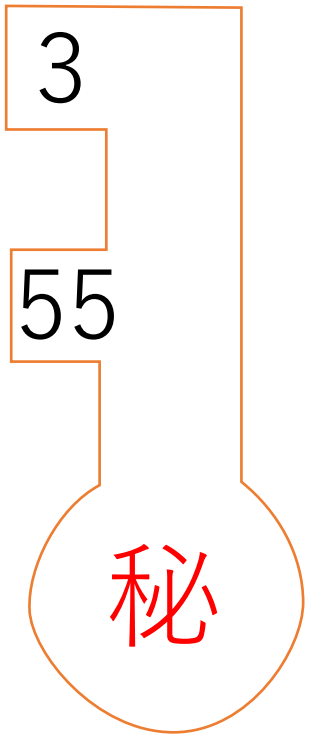


RSA暗号

ただ、積の数が大きいと、何と何の積かすぐには求まりません

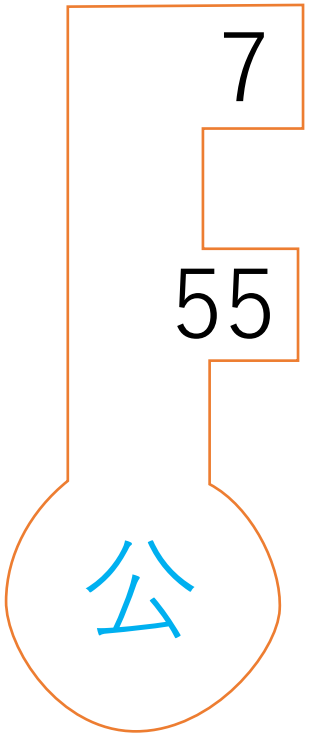
1977年に129桁の合成数で出した問題を、1994年スーパーコンピューターで45時間かけて解読していますが、RSA暗号の安全性が証明されたといっていいかもしれません。

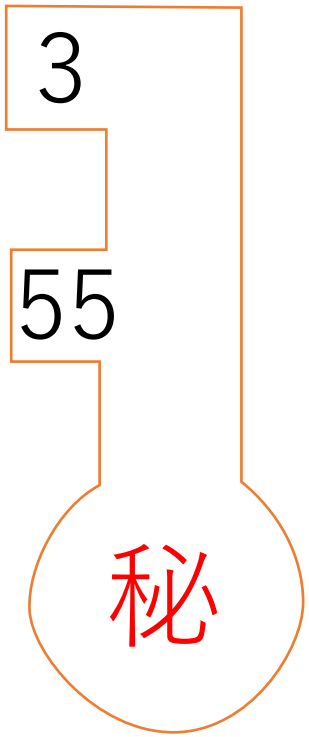




RSA暗号

近年、高速に処理できる量子コンピュータが登場し、実用化すれば、この積を出す数がすぐに求まって、暗号が破られてしまうのではないかという話があります。しかし実用化には時間がかかりそうですので、しばらくは大丈夫でしょう。また、別の暗号化方式も開発されています。





量子コンピュータによる暗号解読の可能性 | NTTデータ (nttdata.com)