KIDS-RSA 暗号（簡単な公開鍵暗号）

鍵の作り方

1. 2 つの整数 a,b を決めます。　　a=　　b=

2　M=ab-1 を計算します。　　M=

3. さらに 2 つの整数 a’ , b’ を決めます。　a’=　　b’=

4. e=a'×M+a を計算します。　　e=　　（公開鍵）

5. d=b'×M+b を計算します。　　d=　　（秘密鍵）

6. n=(ed-1)/M を計算します。　　n=　　（公開鍵）

n と e を公開し、d を自分だけの秘密にします。

「メッセージを暗号化する方法」

送信者はメッセージm（n 未満の自然数）を決めます。mに送る相手の公開鍵 e を掛け、さらに相手の公開鍵 n で割ります。その余り c を暗号文として伝えます。

メッセージm　相手の公開鍵 e　　相手の公開鍵 n　　me を n で割った余り

□ × □ mod □ = □ ←暗号文 C

「暗号文を復号する（もとのメッセージに戻す）方法」

受信者は受け取った暗号文 c に自分の秘密鍵 d を掛け、さらに自分の公開鍵 n で割ります。その余りがもとのメッセージmとなります。

暗号文 c　　自分の秘密鍵 d　　自分の公開鍵 n　　cd を n で割った余り

□ × □ mod □ = □ ←もとのメッセージ

----------キ-------リ-------ト-------リー(公開用)----------

□ の公開鍵　e=　　n=　　.