RSA 暗号の実習

2 人組で片方が送信者，片方が受信者になります。授業用サイトの「第 3 節　情報セキュリティ」から「RSA 暗号」のページに行き，それぞれの役割のページに進みなさい。

○受信者の作業
　p,q,e をそれぞれ違った値に設定して「鍵生成」ボタンを押しなさい。秘密鍵 d が生成されるので，それは秘密にしておいて，公開鍵 n,e の値を下の欄に記入して，送信者に渡しなさい。

n＿＿＿＿＿＿＿＿　e＿＿＿＿＿＿＿＿

○送信者の作業
　n と e の値を自分のページのそれぞれの欄に入力しなさい。英字 5 文字以内の単語を決めて，平文欄に入力しなさい。「暗号化」ボタンを押すと暗号文が生成される。それを下の欄に記入して，受信者に渡しなさい。

暗号文＿＿＿＿＿＿＿＿

○受信者の作業

　画面右側の復号のところに n と d の値を入力し，暗号文を暗号文欄に入力しなさい。「復号」ボタンを押すと復号されるので，できた平文を下の欄に書き，それが正しいかを送信者に見せて確認しなさい。

平文＿＿＿＿＿＿＿＿

参考：送信者の画面で平文は 27 進法（A→1，B→2，…）で数値化されて「平文の数値化」の値になる。これがプリント 39 ページの m であり，m^e を n でわった余り c が「数値の暗号化」欄の値，それを 27 進法の逆でアルファベットに直したのが「暗号文」になっている。
受信者の画面でも同じように 27 進法で文字列と数値を変換している。