RSA 暗号を文字列に適用する場合の処理の流れ

例として暗号化鍵は $(e, n) = (3, 55)$ 復号鍵 $(d, n) = (27, 55)$ の場合にメッセージ文字列 ”Hello” を RSA により暗号化，復号処理を行う手順を示す．

まずメッセージ文字列のそれぞれの文字を文字コードに従って変換し，順に連結した 2 進系列を得る．半角英語の場合，”H” のアスキー符号による 8bit 表現は ”01001000”, ”e” は ”01100101”, ”l” は ”01101100” ”o” は”01101111” なので以下の系列を得る．

$$\text{”Hello”} \rightarrow \text{”0100100001100101011011000110110001101111”}$$

文字，画像などどんなデジタルデータでも一旦 2 進系列になればここから先の処理は同じである．

この例では法を 55 とした演算を行うが，この場合使える数値は 0 から 54 の 55 種類である．しかし，0, 1 はどの鍵で暗号化しても自分自身となる．暗号文が 0, 1 であれば鍵に関わらず平文がそれぞれ 0, 1 だとわかるため 0, 1 は平文として使用できない．このため，使用できる数値は 2 から 54 の 53 個である．5bit をこの数値の一部に割り当てる．ここでは 00010 から 11111 を それぞれを整数の 2 進表記とみたときの数値である 2 から 31 に割当て，0 と 1 が使えない問題を回避するために 00000 を 32 に，00001 を 33 に割り当てる．この約束事も通信相手と事前に共有しておく必要がある．

次に平文を変換した 2 系列を 5bit づつ上記約束事に従って整数系列に変換する．平文のビット系列の長さが 5 の倍数でないときは 5 の倍数になるようにビットを追加する必要があるが，この追加方法の約束事も事前に決めておく必要がある．

$$\text{”0100100001100101011011000110110001101111”} \rightarrow \text{”9, 33, 18, 22, 24, 27, 3, 15”}$$

この系列の要素それぞれに RSA の暗号化関数を施して暗号文系列を得る．（いずれも mod 55 の演算）

$$9^3 \equiv 14, 33^3 \equiv 22, 18^3 \equiv 2, 22^3 \equiv 33, 24^3 \equiv 19, 27^3 \equiv 48, 3^3 \equiv 27, 15^3 \equiv 20$$

送信者は暗号文である整数の系列

$$\text{”14, 22, 2, 33, 19, 48, 27, 20”}$$

を受信者に送る．受信者は逆に，

1. 整数系列である暗号文の要素をそれぞれ RSA の復号関数を施して，整数系列

   $$14^{27} \equiv 9, 22^{27} \equiv 33, 2^{27} \equiv 18, 33^{27} \equiv 22, 19^{27} \equiv 24, 48^{27} \equiv 27, 27^{27} \equiv 3, 20^{27} \equiv 15$$

   を得る

2. 上記系列を約束事に従ってそれぞれを 5bit ずつの系列に変換し 2 進系列

   $$\text{”9, 33, 18, 22, 24, 27, 3, 15”} \rightarrow \text{”0100100001100101011011000110110001101111”}$$

   を得る．

3. これを 8bit ごとに ASCII コードとして解釈し，文字列

   $$\text{”Hello”}$$

   を得る

という手順で元の文字列を得る．