RSA 暗号

RSA 暗号による通信の原理

受信者は，公開鍵 k, m を公開する。

送信者は，平文(plain text)P に対し，$C \equiv P^k \bmod m$ によって暗号文(cipher text) C を作成し，受信者に送る。

受信者は，秘密鍵 u を用いて $C^u \bmod m$ を計算して，平文 P を得る。

公開鍵と秘密鍵の条件

（１） 指定範囲内の任意の P に対し $P^{ku} \equiv P \pmod m$ （復号できること）

（２） k, m から u を容易には推測できないこと。 （暗号の安全性）

公開鍵と秘密鍵をどう作るか。

平文 P として許容する限界より大きい素数 2 個 p, q を用意し，$m=pq$ とする。

$\phi(m)=(p-1)(q-1)$と互いに素な正の整数を選び，公開鍵 k とする。

$ku \equiv 1 \pmod{\phi(m)}$ となる正の整数 u を秘密鍵とする。

復号できる理由

$ku=\phi(m)v+1$ (v は正の整数) とする。

オイラーの定理から，$P^{\phi(m)} \equiv 1 \pmod m$

両辺を v 乗して， $P^{\phi(m)v} \equiv 1 \pmod m$

両辺に P を乗じて， $P^{\phi(m)v+1} \equiv P \pmod m$

$ku=\phi(m)v+1$ より $P^{ku} \equiv P \pmod m$

秘密鍵の安全性

$\phi(m)$が分かれば秘密鍵 u は簡単に求まるけれど，m を素因数分解して p,q を求めるのに時間がかかるので$\phi(m)$を求めるのは容易ではない。

実践（準備）

平文の範囲を 1～10 とする。

10 より大きい素数を 2 個選び，p, q とする。たとえば，$p=17$, $q=13$。

$m=pq$ とし，$\phi(m)=(p-1)(q-1)$と互いに素な正の整数 k を選び，k と m を公開する。

$m=221$，$\phi(m)=16\times12$，$k=11$。

$ku \equiv 1 \pmod{\phi(m)}$ となる正の整数 u を求め（一次不定方程式 $ku-\phi(m)v=1$ の解 u,v を求める），秘密鍵として所持する。$u=35$

公開鍵 $k=11$, $m=221$， 秘密鍵 $u=35$。

暗号文の作成

送信者は，送りたい数 P に対し，$C \equiv P^k \bmod m$ を計算して C を受信者に送る。

暗号文の復号

受信者は，受け取った C に対し，$C^u \bmod m$ を計算する。

実践

（1） P=1，2，3，…，10 に対し，$C=P^k \bmod m$ を計算する。

（2）上記で得た各 C に対し，$C^u \bmod m$ を計算する。

P	$C=P^{11} \bmod 221$	$C^{35} \bmod 221$
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

暗号破り

公開鍵 k，m は傍受者も知りえる。

m を $m=pq$ の形に素因数分解し，秘密鍵 u を計算すると暗号を解読できる。

RSA 暗号の有効性の根拠

大きい数の素因数分解は時間がかかる。

エラトステネスの篩

2 より大きい 2 の倍数，3 より大きい 3 の倍数，5 より大きい 5 の倍数，…　を順に消していくと，素数が残る。

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	96	87	88	89	90
91	92	93	94	95	96	97	98	99	100