

鍵共有法について

秘密鍵共有プロトコル

- AさんとBさんの間で、暗号通信に使う鍵を決めたい。ただし、2人の通信は盗聴されている。どうすればよいか？



巡回乗法群と原始元

- べき乗の計算を p を法とする剰余類で考えてみる

$$y = 5^x \pmod{11}$$

x	1	2	3	4	5	6	7	8	9	10
y	5	3	4	9	1	5	3	4	9	1

$$y = 2^x \pmod{11} \quad \rightarrow 2 \text{ は、法 } 11 \text{ のもとで原始元である}$$

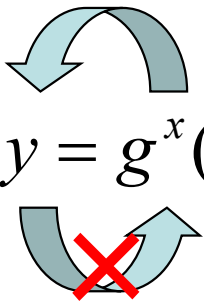
x	1	2	3	4	5	6	7	8	9	10
y	2	4	8	5	10	9	7	3	6	1

F_p の原始元を g とすると、 $1 \sim p-1$ の数は全て g^j の形で表せる

$$g^{p-1} = g^0 = 1 \pmod{p} \text{ に注意}$$

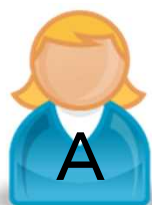
離散対数問題

- 大きな素数 p (10進数で300桁以上)を法とするとき:


$$y = g^x \pmod{p}$$

- x から y を計算するのは(計算機では)簡単
- 一方、 y から x を計算するのは(世界最高速の計算機でも)時間がかかり過ぎて難しい(準指数時間)

Diffie-Hellman(DH)鍵共有法



A

(準備) 大きな素数 p と原始元 g を決める



B

(1) 乱数 a を決める

(2) $y_A = g^a \pmod{p}$
を計算する

(3) y_A を送る



(4) y_B を送る

(1') 乱数 b を決める

(2') $y_B = g^b \pmod{p}$
を計算する

(5') $K' = y_A^b \pmod{p}$
を計算する

(5) $K = y_B^a \pmod{p}$
を計算する

$$K = y_B^a = (g^b)^a = g^{ab} = (g^a)^b = y_A^b = K' \pmod{p}$$

$K=K'$ であり、同じ鍵の値が共有できた！

公開鍵暗号による鍵共有方式

