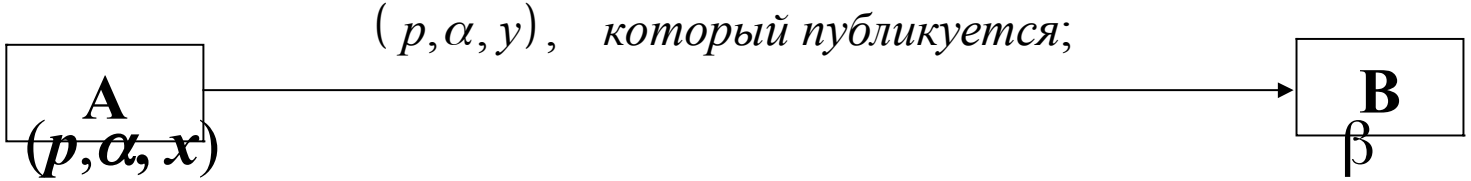
Шифрование с открытым ключом по алгоритму Эль-Гамаля.



Что делает абонент А?

1) **Выбирает большое простое целое число *p* с помощью датчика простых чисел;**
2) **Выбирает примитивный элемент α** $(2 \le \alpha \le p-2)$;
3) **Выбирает случайное число *x – секрет абонента А, 1*** $\le x \le p-1$, т.е. его закрытый ключ $ЗК_A = x = D_A$;
4) **Вычисляет** $y = \alpha^x \pmod p$;
5) **Создает свой открытый ключ** $ОК_A = E_A = (p,\alpha,y)$, *который публикуется*;

Шифрование абонентом **В** на открытом ключе абонента **А** по алгоритму Эль-Гамаля

Абонент В:

1) Извлекает открытый ключ абонента **А:**

$$ОК_A = (p, \alpha, y) = (p, \alpha, y = \alpha^x),\ где\ x - секрет\ A.$$

2) Формирует сообщение MЄ[1,p–1];

3) Выбирает случайное число β, [1,p–1];

4) Вычисляет два числа: $a = \alpha^{\beta} \pmod p$; $b = M \cdot y^{\beta} \pmod p$;

5) Создает шифрованное сообщение С: C=(a,b) и отправляет А

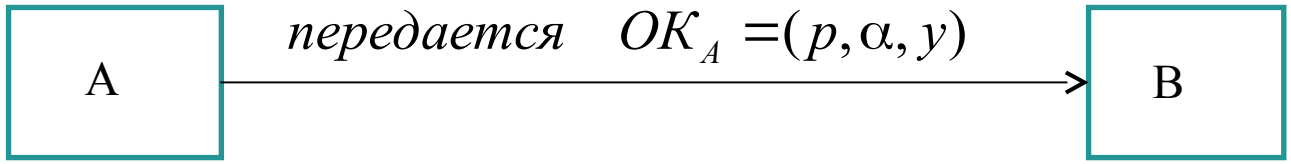
Расшифровка на стороне А:

1) Используя $ЗК_A = x$, вычисляет

$$\frac{b}{a^x} = \frac{M \cdot y^{\beta}}{(\alpha^{\beta})^x} = \frac{M(\alpha^x)^{\beta}}{\alpha^{\beta x}} = M \pmod p.$$

Рассмотреть пример: p=13, x=7, β=8, M=4.

Электронная цифровая подпись по алгоритму Эль-Гамаля



$ЗК_A = x$ - *простое число*, $\in [1, p-1]$;

$ОК_A = (p, \alpha, y)$, *где* $y = \alpha^x \pmod p$;

$\beta \in [1, p-1]$ – взаимно простое с (p-1)

Абонент А: Сообщение - “m”;

Вычисляется хеш от передаваемого сообщения h=H(m) mod(p-1)

Находит два числа a и b: $a = \alpha^{\beta} \pmod p$; $b = \dfrac{h - x \cdot a}{\beta} \bmod (p-1)$;

Сообщение подписывается зашифрованной подписью $S(m)=(a,b)$

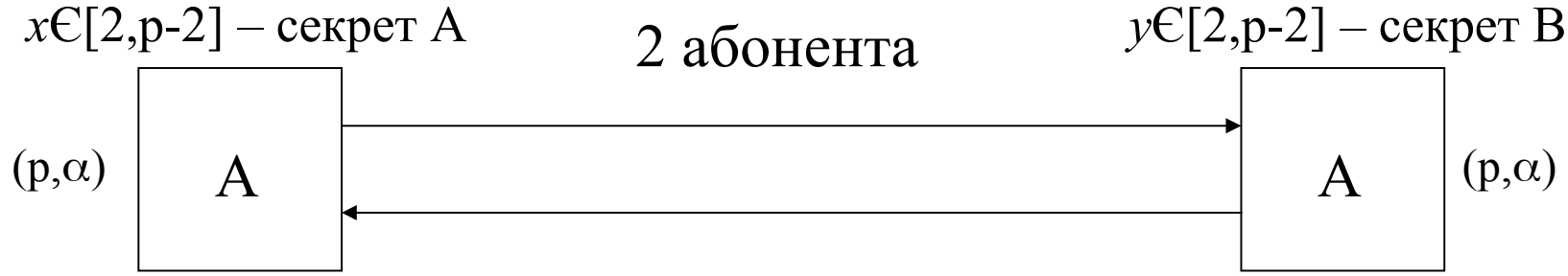
И передается абоненту В сообщение с шифрованной подписью $(m, S(m))$.

Абонент В вычисляет по принятому сообщению хеш: h=H(m) mod(p-1)

На стороне В:

$f_1 = \alpha^h \pmod p$; $f_2 = y^a \cdot a^b = (\alpha^x)^a \cdot a^b = (\alpha^x)^a \cdot (\alpha^{\beta})^{\frac{h - xa}{\beta}} = \alpha^h \pmod p$; *т.е.* $f_1 = f_2$.

Системы с общим секретным ключом по протоколу Диффи-Хеллмана (1976)



p – большое простое число;

α – примитивный элемент.

$$\alpha^{p-1} \equiv 1 \bmod p$$

1) Обмен: $A \to B: \quad \alpha^x \pmod p$; $\qquad B \to A: \quad \alpha^y \pmod p$;

2) A формирует ключ: $K_A = (\alpha^y)^x \bmod p$;

3) B формирует ключ: $K_B = (\alpha^x)^y \bmod p$;

Получается одинаковый, т. е. **общий секретный ключ**: $К_А = К_В = К$

Рассмотреть пример: $p=7$; $x=2$; $y=5$.

3 абонента (протокол Диффи-Хеллмана)

x y z

A, B, C

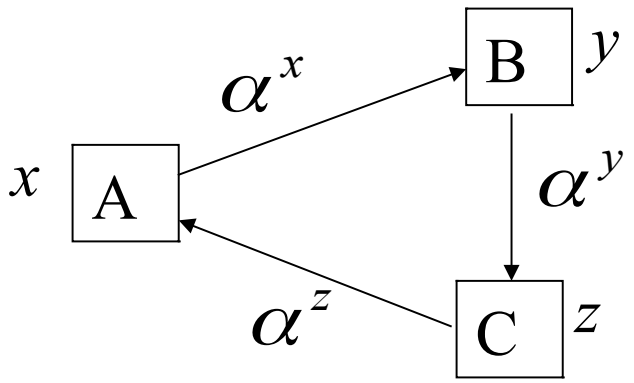
(p,α)

1-ый раунд:

$A \to B: \quad \alpha^x \bmod p;$

$B \to C: \quad \alpha^y \bmod p;$

$C \to A: \quad \alpha^z \bmod p.$

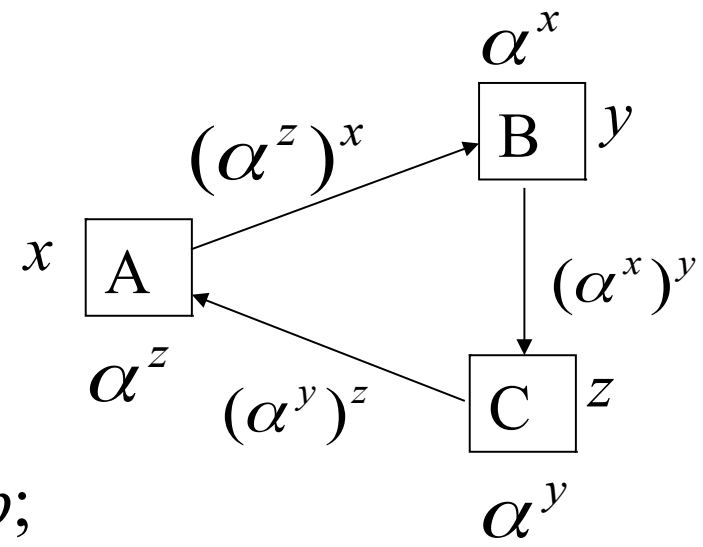


2-ой раунд:

$A \to B: \quad (\alpha^z)^x \bmod p;$

$B \to C: \quad (\alpha^x)^y \bmod p;$

$C \to A: \quad (\alpha^y)^z \bmod p.$



3-ий раунд:

$A \to B: \quad K_A = (\alpha^{yz})^x = \alpha^{xyz} \bmod p;$

$B \to C: \quad K_B = (\alpha^{zx})^y = \alpha^{xyz} \bmod p;$

$C \to A: \quad K_C = (\alpha^{xy})^z = \alpha^{xyz} \bmod p.$

Общий сеансовый ключ: $К_А = К_В = К_С = К$