Криптография с открытым ключом

Проблема распределения ключей

- Какое количество ключей необходимо для общения двух человек? 5? 100? 1000?

Однонаправленные функции

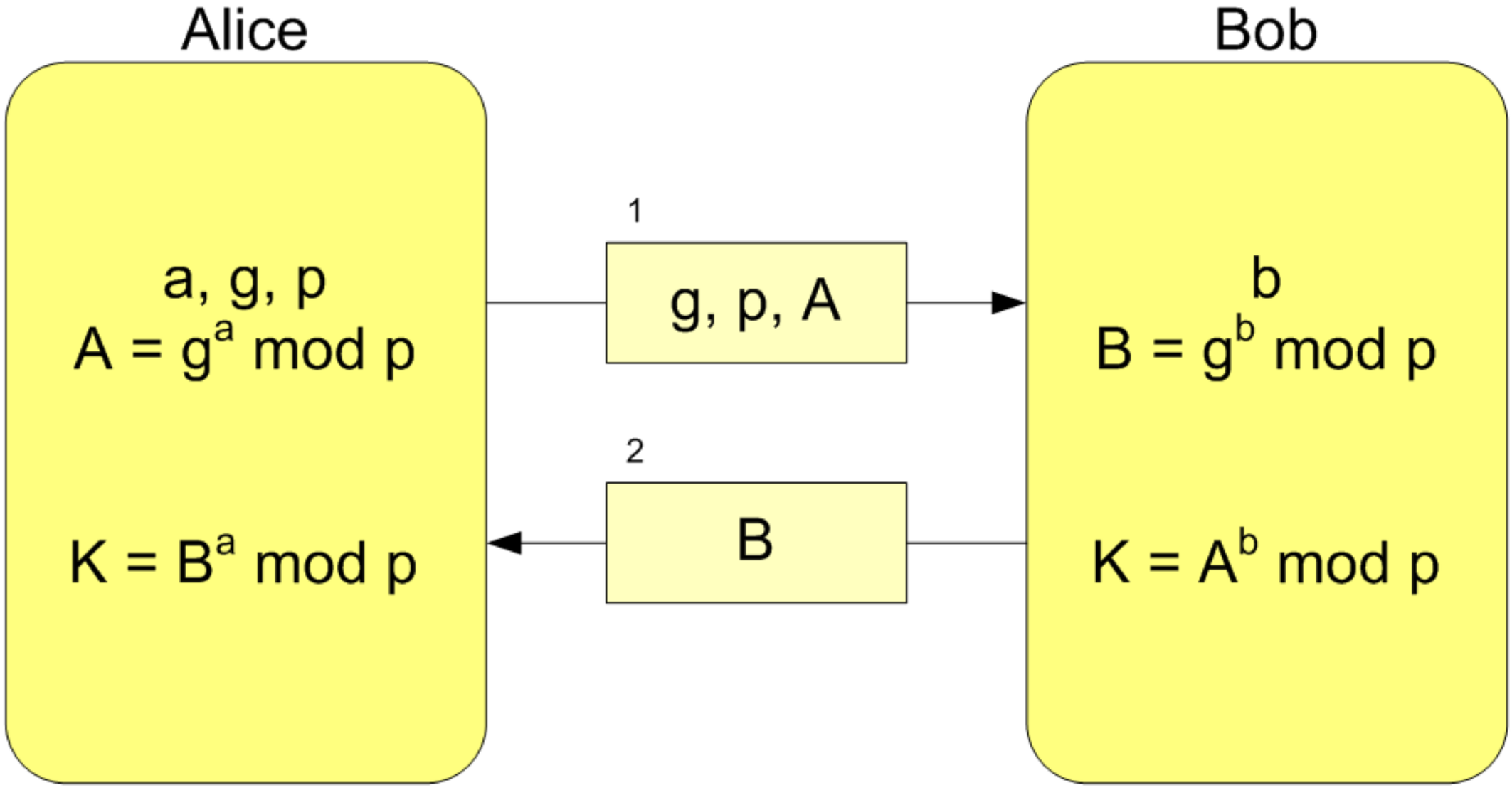
Однонаправленными (односторонними) функциями называются такие, которые *легко* вычислить, но *сложно* обратить

Подтверждает, что P≠NP

Функции *с лазейкой* (trapdoor functions)

Diffie-Hellman

Diffie-Hellman



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

RSA

RSA

1. Выбираются два случайных простых числа p и q заданного размера (например, 1024 бита каждое).
2. Вычисляется их произведение n = pq, которое называется модулем.
3. Вычисляется значение функции Эйлера от числа n φ(n)=(q-1)(p-1)

RSA

1. Выбирается целое число e (), взаимно простое со значением функции φ(n).

- Число e называется открытой экспонентой (англ. public exponent)
- Время, необходимое для шифрования с использованием быстрого возведения в степень, пропорционально числу единичных бит в e.
- Слишком малые значения e, например 3, потенциально могут ослабить безопасность схемы RSA.

RSA

- Вычисляется число d, мультипликативно обратное к числу e по модулю , то есть число, удовлетворяющее условию $de \equiv 1 \pmod{\varphi(n)}$ или $de = 1 + k\,\varphi(n)$, где k — некоторое целое число.
  - Число d называется секретной экспонентой.
  - Обычно, оно вычисляется при помощи расширенного алгоритма Евклида.

RSA

- Пара P = (e,n) публикуется в качестве открытого ключа RSA
- Пара S = (d,n) играет роль секретного ключа RSA

RSA, шифрование

- Шифрование на открытом ключе (e, n)
  - Открытый текст M
  - Шифротекст $C = M^e \bmod n$

RSA, расшифровка

- Расшифровка за закрытом ключе (d, n)
- $C^d \bmod n = (M^e \bmod n)^d \bmod n = M^{ed} \bmod n = M \bmod n$

Сравнительная стойкость

Необходимо сравнить стойкость ключей

- Строгой оценки нет
- Оценивается вычислительная сложность известных атак
  - на процессорах общего назначения и на специальном оборудовании
- Критерий Ленстры

Сравнительная стойкость

	Симметричное	Ассиметричное		Хеш
		Оптимистично	Пессимистично	
2008	74	1062	1077	147
2009	74	1087	1114	148
2010	75	1112	1152	150
2011	76	1138	1190	151
2012	76	1164	1229	152

Упражнение

- Установить gpg, создать ключи