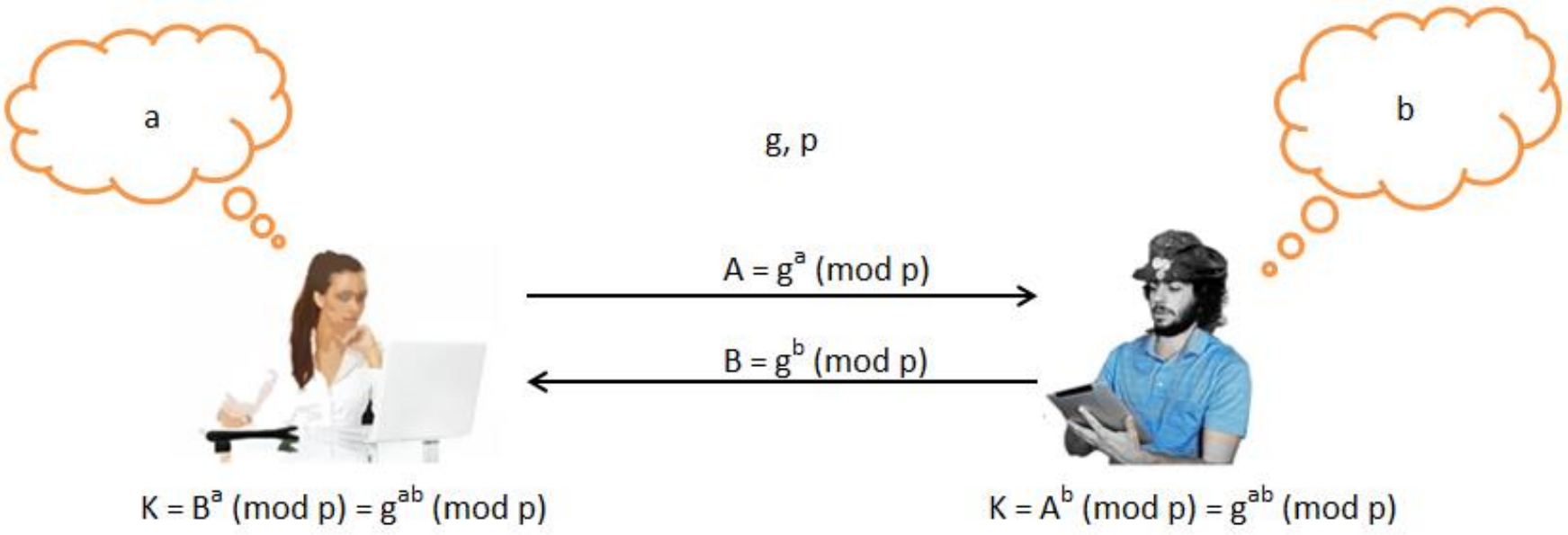
Информационная безопасность

Криптографические протоколы

(презентация к лекции 5)

Амелин Р. В. Информационная безопасность. Конспект лекций // Амелин Р.В. Лаборатория преподавателя [Электронный ресурс]. URL: rv-lab.ru (2017).

Протокол Диффи-Хеллмана



- **p –** очень большое простое число
- **q** – целое число; q ∈ {1 … p}. Обычно выбирается первообразный корень по модулю p: такое число, что $g^{\varphi(p)} = 1 \pmod p$ и $g^l \neq 1 \pmod p$ для всех $l < \varphi(p)$
- q и p являются общеизвестными, либо могут генерироваться первой стороной и отправляться вместе с A
- числа a и b выбираются сторонами случайно: a,b ∈ {1, …, p-1}

Протокол Диффи-Хеллмана

g, p, B, A

K = ?

- **Задача дискретного логарифмирования**: дано p – простое число, a – порождающий элемент группы F_p^* и b $\in F_p^*$. Найти такое x, что $a^x \pmod p = b$. Известно, что решение существует и единственно.
- Эффективный алгоритм решения этой задачи неизвестен. Существующие алгоритмы базируются на полном или частичном переборе элементов группы F_p^*
- Устойчивость протокола Диффи-Хеллмана базируется на сложности задачи дискретного логарифмирования

Протокол Диффи-Хеллмана

Атака «человек посередине»