МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования

**«Московский технический университет связи и информатики»**

Кафедра «Информатика»

Лабораторная работа №1

**по дисциплине**

**«Информационная безопасность»**

Выполнил: студент гр. БЭИ2202

Кулешов А.С.

Москва, 2024 г

Начну выполнение заданий 14, 38, 62

1. Опишите поведение полиморфных вирусов.

Полиморфные вирусы - вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите.

Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика.

Полиморфизм заключается в формировании программного кода вредоносной программы «на лету» — уже во время исполнения, при этом сама процедура, формирующая код, также не должна быть постоянной и видоизменяется при каждом новом заражении. Зачастую, изменение кода достигается путём добавления операторов, не изменяющих алгоритм работы программного кода (например, оператор NOP).

Постоянное видоизменение программного кода вредоносной программы не позволяет создать универсальную сигнатуру для данного образца вредоносной программы. На сегодняшний день для противодействия данному методу в антивирусном программном обеспечении применяются такие технологии, как эвристический анализ и эмуляция.

1. В чём состоит смысл метода экспоненциального обмена?

Метод экспоненциального обмена - метод установления секретного ключа шифрования, в котором каждый авторизированный пользователь канала влияет на его значение. Является симметричным методом.

Недостатком симметричных криптосистем является сложность передачи ключа. Необходим защищенный канал, по которому осуществится начальный обмен ключом. Если две стороны не могут установить безопасный начальный обмен, существует риск перехвата сообщений третьей стороной. Далее будет описан протокол Диффи-Хеллмана.

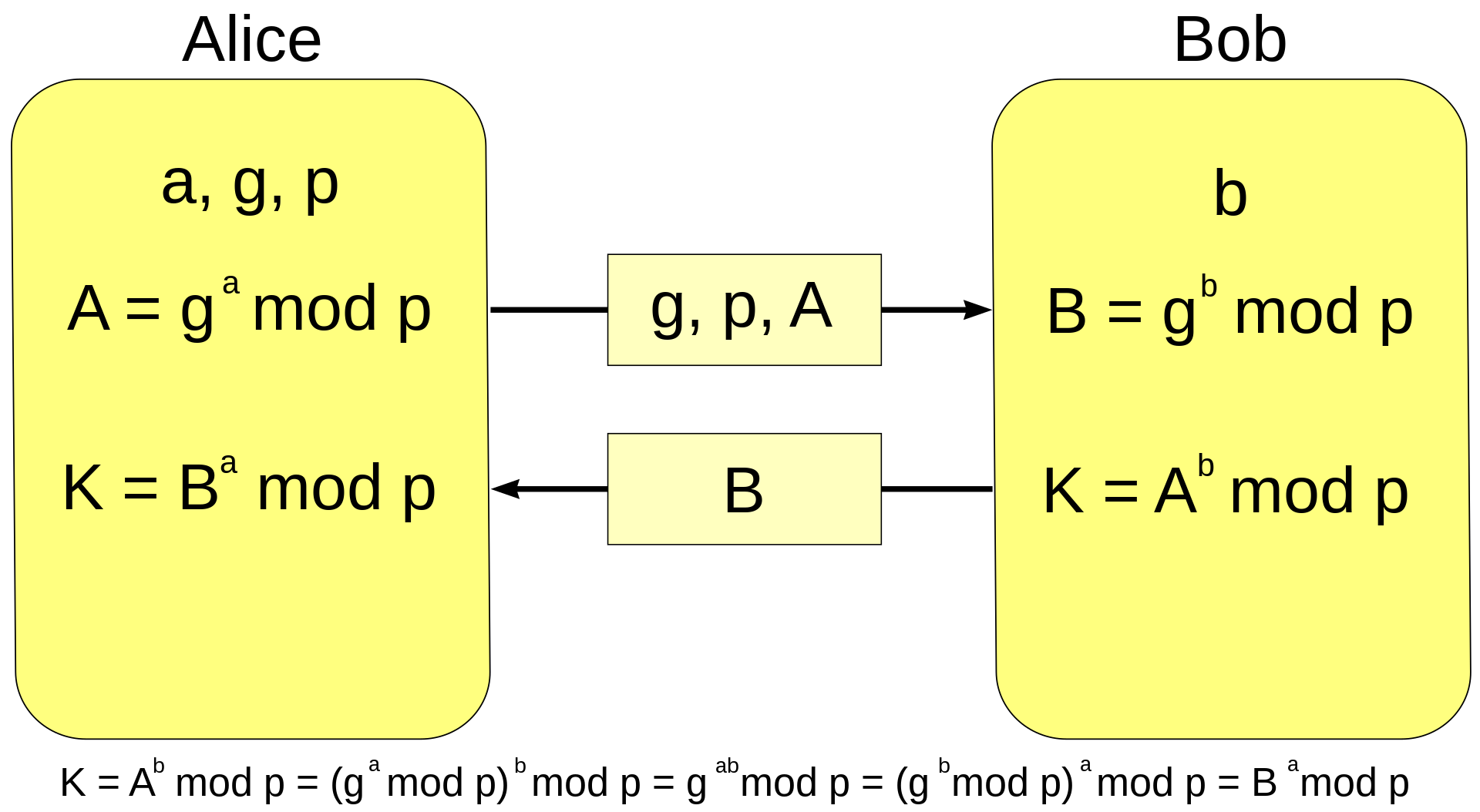


Рисунок 1 – краткая демонстрация протокола

При работе алгоритма каждая сторона:

1. генерирует случайное натуральное число *a* — *закрытый ключ*
2. совместно с удалённой стороной устанавливает *открытые параметры* *p* и *g* (обычно значения *p* и *g* генерируются на одной стороне и передаются другой), где

*p* является [случайным простым числом](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D1%87%D0%B0%D0%B9%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE)

*(p-1)/2* также должно быть [случайным простым числом](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D1%87%D0%B0%D0%B9%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE) (для повышения безопасности)[[5]](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%94%D0%B8%D1%84%D1%84%D0%B8_%E2%80%94_%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%D0%B0#cite_note-5)

*g* является [первообразным корнем](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B2%D0%BE%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D1%80%D0%B5%D0%BD%D1%8C_(%D1%82%D0%B5%D0%BE%D1%80%D0%B8%D1%8F_%D1%87%D0%B8%D1%81%D0%B5%D0%BB)) [по модулю](https://ru.wikipedia.org/wiki/%D0%A1%D1%80%D0%B0%D0%B2%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E) *p (также является простым числом)*

1. вычисляет *открытый ключ* *A*, используя преобразование над *закрытым ключом*

*A = ga*mod*p*

1. обменивается *открытыми ключами* с удалённой стороной
2. вычисляет *общий секретный ключ* *K*, используя открытый ключ удаленной стороны *B* и свой закрытый ключ *a*

*K = Ba*mod*p*

*К* получается равным с обеих сторон, потому что:

*Ba*mod*p = (gb*mod*p)a*mod*p =****gab*mod*p****= (ga*mod*p)b*mod*p = Ab*mod*p*

В практических реализациях для *a* и *b* используются числа порядка 10100 и *p* порядка 10300. Число *g* не обязано быть большим и обычно имеет значение в пределах первого десятка.

1. Категории фагов, описание?

Программы-фаги (сканеры) используют для обнаружения вирусов метод сравнения с эталоном, метод эвристического анализа и некоторые другие методы. Программы-фаги осуществляют поиск характерной для конкретного вируса маски путем сканирования вначале в оперативной памяти, а затем в файлах и при обнаружении выдают соответствующее сообщение.

Программы-фаги не только находят зараженные вирусами области памяти и файлы, но и «лечат» их (то есть удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние). Среди фагов выделяют полифаги – программы-фаги, предназначенные для поиска и уничтожения большого числа вирусов.

Программы-фаги делятся на две категории:

1. универсальные сканеры, осуществляющие поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер;
2. специализированные сканеры, предназначенные для обезвреживания ограниченного числа вирусов или только одного их класса, например макровирусов.

Программы-фаги также делятся на:

* резидентные мониторы, производящие сканирование «на лету» и обеспечивающие более надежную защиту системы, поскольку они немедленно реагируют на появление вируса;
* нерезидентные сканеры, обеспечивающие проверку системы только по запросу и способные опознавать вирус только во время своего очередного запуска.

Достоинство программ-фагов всех типов – их универсальность. Недостатки – относительно небольшая скорость поиска вирусов и большие размеры антивирусных баз, которые сканерам приходится хранить и пополнять.