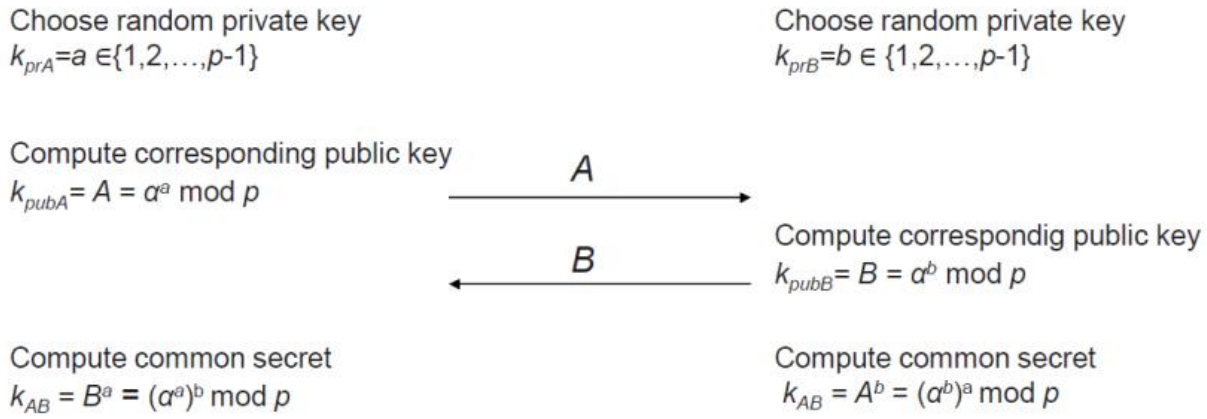
Домашна задача бр.5
Криптографија

Diffie-Hellman key exchange protocol

Стефан Андонов, 151020
stefan.andonov@students.finki.ukim.mk

Функционирање на DHKE Протоколот

DHKE протоколот функционира според следните чекори:
Нека имаме две страни (A и B) кои што сакаат да комуницираат помеѓу себе со шифрирани пораки користејќи некој од познатите алгоритми за симетрична криптографија.
1. Се избираат јавни параметри:
- *p* – голем прост број
- g (или α) – број којшто се наоѓа помеѓу 2 и бројот *p*
2. Се објавуваат јавно параметрите p и g.
3. Двете страни кои што комуницираат меѓу себе си одбираат свои тајни вредности *a* и *b*. Потребно е *a* и *b* да се помали од *p*.
4. Понатаму постапката на генерирање на јавните клучеви на A и B, како и на заедничкиот таен клуч, којшто ќе се користи во криптирањето на пораките со некој алгоритам за симетрична криптографија, е следната:



Програмска имплементација на DHKE протоколот

Имплементацијата на протоколот ќе ја прикажам со помош на програмскиот јазик Java. Истата е достапна на мојот профил на GitHub.

Имплементацијата е составена од 4 класи и тоа:
- DHKEProtocolPublic – wrapper класа во која што се чуваат јавните параметри p и g,
- DHKEProtocolA и DHKEProtocolB, класи кои ги претставуваат двете страни кои комуницираат A и B, и во кои тие избираат тајни параметри a и b, како и ги

генерираат своите јавни клучеви, и заедничкиот таен клуч којшто би се користел како клуч за симетрична криптографија

Воспоставување на заеднички клуч и размена на пораки

Заедно со колешката Ивана Срњакова, ги избравме следните параметри за DHKE протоколот:

- p = 2,038,074,743 (31-битен)
- g = 1000

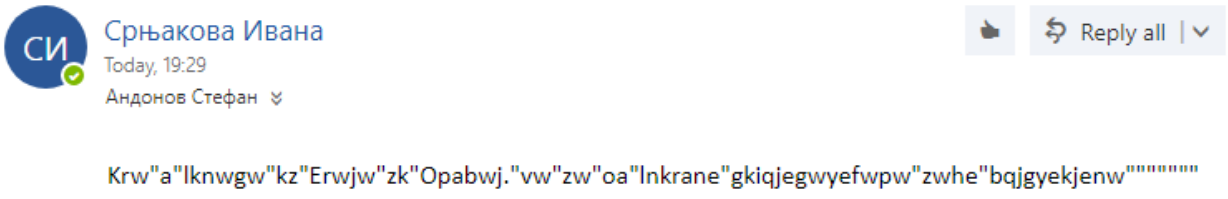
Потоа, колешката ја одбира страната на Alice и ја користи класата DHKEProtocolA, додека пак јас ја одбирам страната на Bob, и ја користам класата DHKEProtocolB.

За моја вредност на b ја одбирам b=7, па со тоа, јавниот клуч којшто јас го објавувам B=159,047,246.

Јавниот клуч којшто колешката го објави е A = 2007280509, па според тоа тајниот клуч којшто го генерирав е $К_{sec}$=224709026.

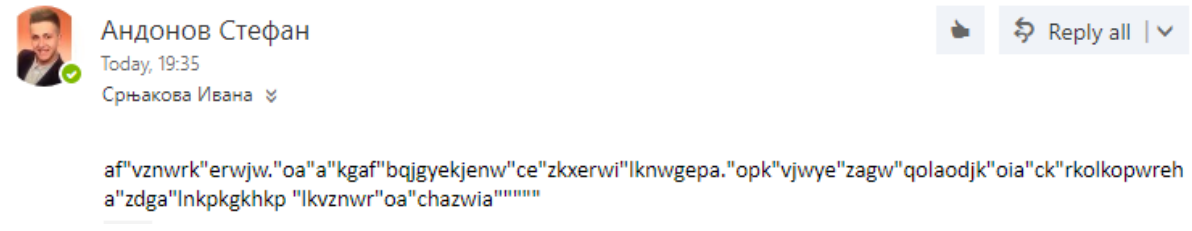
Алгоритамот којшто ќе го користиме за симетрична криптографија е истиот што го имав дизајнирано за потребните на 4тата лабораториска вежба, односно блок шифрувач со големина на блок од 64 бита (8 ASCII карактери), и клуч некој број со максимална големина 64 бита.

1. Пораката која што ја добив од колешката е следната:



2. Пораката ја декриптирав со клучот 224709026 и го добив следното:
`Ova e poraka od Ivana do Stefan, za da se proveri komunikacijata dali funkcionira.`

3. Потоа јас и ја испратив пораката:
`ej zdravo ivana, se e okej funkcionira gi dobivam porakite, sto znaci deka uspeshno sme go vospostavile dhke protokolot. pozdrav se gledame`
Истата је енкриптирав со истиот клуч пред да ја пратам:



Овие активности ги реализирав во кодот од 4тата лабораториска вежба со измени во main функцијата на класата BlockChiperTest.java и истие се ажурирани на github.

Напад на DHKE протокол

Всушност напад на овој проток означува напад на дисректниот логаритамски проблем (DLP), којшто се смета за исклучително тежок, за огромни броеви. Целта е да се најде решението (вредноста на x) во равенството $\alpha^x = \beta \ (mod\ p)$.

Начините за да се постигне истото е со следните алгоритми:

- brute force (O(p))
- Shank's Baby Step Giant Step (O($\sqrt{p}$))
- Pollard's Rho (O($\sqrt{p}$))

Во мојата имплементација достапна на GitHub, имплементиран е алгоритмот BabyStepGiantStep, со посебна класа за тоа.

Целта е, доколку има натрапник во средината на комуникацијата меѓу Alice и Bob, откако тој ќе ги види јавните параметри p и g, и откако ќе го пресретне јавниот клуч на Alice, да го реши дискретниот логаритамски проблем и да го најде тајниот експонент a на Alice, па потоа откако ќе го прими и јавниот клуч на Bob, B, да го изгенерира нивниот заеднички таен клуч.

Ова се постигнува со помош на функцијата:

```
public static BigInteger logBabyStepGiantStep(BigInteger base, BigInteger residue, BigInteger modulus)
```

За да ја истестирам функцијата, ја повикав со параметрите:
base = g (јавниот параметар)
residue = A (јавниот клуч на Ивана)
modulus = p (јавниот параметар)

По извршување на програмата, за многу брзо време (поради малите вредности на p и на g), се доби резултатот дека тајниот параметар на Ивана a = 9.

Потоа на мојот јавен клуч B = 159,047,246, му ја пресметав вредноста на степен a = 9, по модул p, и добив вредност 224709026, која што се совпаѓа со нашиот заеднички таен клуч, со што се покажува успешноста на овој напад.

За да биде комуникацијата отпорна на напад, потребно е p да биде прост број со големина од најмалку 160 бита.