Activitat 06: xifrat asimètric

Introducció

Aquesta activitat pretén introduir el xifratge asimètric en Java, per mostrar un dels mètodes de xifratge més segurs del present, però que pot quedar trencat en un futur per la computació quàntica.

Enunciat

Crea la carpeta 07-Public_key dins del teu repositori a nivell arrel. Tot el projecte que faràs anirà dins d'aquesta carpeta.

Crea un projecte maven en el teu entorn de desenvolupament (busca com fer-ho si no ho has fet mai). El package ha de ser iticbcn.xifratge i el nom del projecte (Artifact id) xifreatgepk, no estereotype → et crearà l'arxiu /07-Public_key/xifratgepk/src/main/java/iticbcn/xifratge/Main.java

Pasos

- Crea la classe `ClauPublica`
- Dins la classe crea el mètode `public KeyPair generaParellClausRSA() throws Exception`
- També crea `public byte[] xifraRSA(String msg, PublicKey clauPublica)throws Exception`
- També `public String desxifraRSA(byte[] msgXifrat, PrivateKey ClauPrivada)`

Notes d'implementació

NOTA: `Main.java` que us dono fa ús d'una llibreria que l'heu d'afegir al `pom.xml`:

```
<dependencies>

<dependency>
<groupId>javax.xml.bind</groupId>
<artifactId>jaxb-api</artifactId>
<version>2.3.1</version>
</dependency>

</dependencies>
```

Codi aportat

La classe `Main.java` té el següent codi:

```
package iticbcn.xifratge;
```

```
import java.security.KeyPair;

import javax.xml.bind.DatatypeConverter;

public class Main {
public static void main(String args[]) throws Exception {

ClauPublica cp = new ClauPublica();

String msg = "Missatge de prova per xifrar áéíóú àèìòù äëïöü";

KeyPair parellClaus = cp.generaParellClausRSA();

byte[] msgXifrat = cp.xifraRSA(msg, parellClaus.getPublic());

System.out.println("================================");
System.out.print("Text xifrat: ");
System.out.println(DatatypeConverter.printHexBinary(msgXifrat));

String msgDesxifrat = cp.desxifraRSA(msgXifrat, parellClaus.getPrivate());
System.out.println("================================");
System.out.println("Text desxifrat: " + msgDesxifrat);

String strClauPub = DatatypeConverter.printHexBinary(
parellClaus.getPublic().getEncoded());

String strClauPriv = DatatypeConverter.printHexBinary(
parellClaus.getPrivate().getEncoded());

System.out.println("================================");
System.out.println("Clau pública: " + strClauPub);
System.out.println("================================");
System.out.println("Clau privada: " + strClauPriv);

}
}
```

Resultat esperat

```
================================
Text xifrat:
5C41B05D11CEE08087D54B33D5E45A4F4CCC6F165F174A4CA2D1274CB97EBBE279DDAF6A24F87439FA5CE5845656615492AA
0188A0A2D398A1C38E9B47C5236F4F71408669526BAEF89FA1A77969DA4D363E4C7D4D127BE15E14D1D50EF083C0D0FDE8CD
159F11E8B509A528CAD4483716A64D7E36E10EF7C2D187DC9A5E81ED83BCD99DC621E6AE0519EB440B708E4B85B3F22E1168
710AA13A35EA132936A5F5F05F355080CE67EA6F2F3FEFD75DEF7D020D1FEBB66C79F69F27D529CF3DC41C596D00EFD22403
0F2A35A98E0F68C0D8B3D67EB5F064113DEE2A1144C6468C44A0F7C230C8E7D15A7F37C9D097D17555B48F2CAB1F3E9357CE
2A0C956E0C47
================================
Text desxifrat: Missatge de prova per xifrar áéíóú àèìòù äëïöü
================================
```

```
Clau pública:
30820122300D06092A864886F70D01010105000382010F003082010A0282010100B4FC2F0EBA8020666C20C25E8539D23861
6608535FAAD07451AB9CEDC8EB35405CA13FDE8B0AF3315C2C2F3A355FEDB51C931E4020815B5D4C481394CE83C9ABC019EB
AAF785BD6E475230D9D4C23C80EE2F5955CDF70E9CD246790605C6259FBFF31D1AB0A4EEAF1BD3CBC11B20444220095542D9
2FC18B687CF9712EFDEA25FBBC69566177B910B87439F5DF4D79EFB86DC71F62042BC59EBD934A95789311A926A41004EF75
18DC27C8C01FD0BA0FA764B5EBE29E8586612181CB7B2FD79F5235D4148CFB670C10D9279717AC299656CC664809ABDDCE7F
F16137F4763BBDB720DC6E4CA5BB14884E9FD4340FE0A299B2439665393859A787C4551918B7890203010001
==================================
Clau privada:
308204BD020100300D06092A864886F70D010101050004820A7308204A30201000282010100B4FC2F0EBA8020666C20C25E
8539D238616608535FAAD07451AB9CEDC8EB35405CA13FDE8B0AF3315C2C2F3A355FEDB51C931E4020815B5D4C481394CE83
C9ABC019EBAAF785BD6E475230D9D4C23C80EE2F5955CDF70E9CD246790605C6259FBFF31D1AB0A4EEAF1BD3CBC11B204442
20095542D92FC18B687CF9712EFDEA25FBBC69566177B910B87439F5DF4D79EFB86DC71F62042BC59EBD934A95789311A926
A41004EF7518DC27C8C01FD0BA0FA764B5EBE29E8586612181CB7B2FD79F5235D4148CFB670C10D9279717AC299656CC6648
09ABDDCE7FF16137F4763BBDB720DC6E4CA5BB14884E9FD4340FE0A299B2439665393859A787C4551918B789020301000102
8201000B1D73C932E13628FDC06CE5E62D5033ECD366A818F7821EDDE0C6C4668C990DBC29043F40EF69EC54075573966AFB
E56A7D248AC37AB181100D27F44E52F97A72ED516736E232E961D158B54CE3D95867BB9A19A63DE35AF46EA628B7077730AB
56B6DBF877E0A460436EBF8C03D5FD56D8F24A0D3803507232A5152684F7CB2BC10FC08A4979BD251C7DBD74E0F5732FE998
2117099D66B28BA9319C86A9C19F0ED49A306186CDFA4C19A24FC803ED203AAC69E169F404F7BD2B992EAE0D42F6CEDA0E6B
7AA34228C96A0C67B6C098C4F87F76680CD1716CD6042EA3620A4A4A34CE78FA2E09182C235C519BF14F37B8EF67A0A09370
3E46850220BE0F95F302818100BE81E6D92E13C1463757A32D4B81C4D8F1B6E6767CE1CF981F2DF626553114B644FA0FC6D0
634A3A1C5AEFF5119E16E1366D0C0A5FA9D5D5BF50860CFB3FAC857DF288A3DF1DFFED9BBFF4C199BC16FC9DD2913F182FD0
87571400AD5C10EF0F204073F1F21CFD0BFF658B003269BF6D9C1193C2C9DF31BE0DFAB988A716277F02818100F3343E8C0E
60D7E46D197B5AB9BDAE4CAB9B84D104C3A3705E5E61BCB712FEF3E3336CF2133B111C35AF74134D66420C8CAC644EAE085E
A010DDDABE35645B8DAF9677339911AB9523C5042F7CDBF5DB3E410265A6DB3ABBA87D72C44FD4C954D19D7C3C6099E5E17A
D6D2C89ACCCC122864B10532DF173524735635F23564F702818075DE215A15EC1B14BA80FA70B7DADE53EB996215C546610E
999BF243DD49B4AAE11A665077F636A2A5908E0E6E8C0553EA3CA5CA754DBB03B88EB5A1AA81C6D80108E209A1AE09FE94F2
BB185D69C63F1DD67E0F2F83C5DD36BF257C1D0E4D1A6AB5F606A7E9CF9670B9FEBA6C7688FDE425EBEA04C4971E23C010B2
BFCE313902818100C85113E390443C0EADBDFB5872FCC4FFE9A922F076981D9A846000E8CB721E050BF2639DD0312A9AADAD
625233C2324CDBE1728D4BD320FD7E66FDB105912FC7B8049B1228D5E119EA6870561CE59FCF81AB522A20111A834EF864FB
4535E2CEB6089D37ADE994EAEF9ED9E6D97A2DEC16D138ED2B458D7BFC15F3C0634B8F69028180229A8944234BD6FEB7AC33
C48BD178E829DF3E7BED48BC21F2B0B9704A8AA8AB3F633FDE0D1FB86F74911277BDFDBFA12326039CC86B094AA4C8E0EF79
D8626DD59AAD575BC9521E2684E39A164C6C60201E682DE9152A9C1C47051071A3E2C772EEC2E9127ACE9F281657F7D8FE9D
5DFA91291D31AEF26FC43D71CC88BE7853
```

Lliurament

Has de lliurar el link al teu repository Github de la UF i el codi de l'activitat ha d'estar dins de la carpeta «`07-Public_key`».