



جامعة دمشق  
كلية الهندسة المعلوماتية  
هندسة برمجيات ونظم المعلومات  
سنة خامسة

## أمن نظم المعلومات

### تقرير تطبيق محاكاة الصراف الآلي ATM

بإشراف:

- م. أريج رحال.

أسماء الطلاب:

- عمر درباع.
- حمزة الطبعي.

## جدول المحتويات

1. المقدمة
2. بنية النظام
3. مجموعة التكنولوجيا
4. تقنيات التشفير المستخدمة
5. خطوات التنفيذ
  - تنفيذ جانب الخادم
  - تنفيذ جانب العميل
6. تصميم قاعدة البيانات
7. لقطات الشاشة وشرح كل مرحلة
8. الخاتمة

## 1. المقدمة

تم تصميم تطبيق محاكاة الصراف الآلي لتوفير بيئة آمنة للتعامل مع المعاملات المالية الحساسة مثل الإيداعات والسحوبات والتحقق من الرصيد. يستخدم التطبيق تقنيات التشفير المتماثل وغير المتماثل لضمان سرية وسلامة بيانات المستخدم أثناء النقل والتخزين. يوضح هذا التقرير عملية التنفيذ والتقنيات المستخدمة وطرق التشفير المطبقة في المشروع.

## 2. بنية النظام

يتبع التطبيق بنية عميل-خادم حيث:

- يستمع الخادم على المنفذ 3000 ويتعامل مع اتصالات العملاء المتعددة في نفس الوقت باستخدام نهج متعدد الخيوط (Multi thread).
- يتفاعل العميل مع المستخدمين، مما يسمح لهم بإجراء المعاملات بأمان.

## 3. مجموعة التكنولوجيا

- جانب الخادم: Nest.js (إطار عمل Node.js)
- قاعدة البيانات: PostgreSQL مع TypeORM
- جانب العميل: JavaScript (للتفاعل)
- التشفير: RSA للتشفير غير المتماثل و AES للتشفير المتماثل.

## 4. تقنيات التشفير المستخدمة

- التشفير غير المتماثل (RSA)

يتم استخدام RSA لتأمين الاتصال بين العميل والخادم. يضمن أن جميع البيانات المتبادلة مشفرة، مما يوفر السرية والسلامة أثناء النقل.

- التشفير المتماثل (AES)

يتم استخدام AES لتخزين بيانات اعتماد المستخدم والمعلومات الحساسة على الخادم بشكل آمن. تتيح هذه الطريقة تشفير وفك تشفير البيانات بسرعة، مما يضمن أنه حتى إذا تم اختراق قاعدة البيانات، تظل المعلومات محمية.

## 5. خطوات التنفيذ

- تنفيذ جانب الخادم

1. إعداد تطبيق Nest.js: بدء مشروع Nest.js وتثبيت الاعتماديات اللازمة بما في ذلك pg للاتصال بـ PostgreSQL و crypto للتشفير.

2. إنشاء نموذج المستخدم: تعريف نموذج مستخدم باستخدام TypeORM للتفاعل مع PostgreSQL.

3. تشفير البيانات: استخدام RSA لتشفير مدخلات المستخدم (طلبات الإيداع والسحب) قبل إرسالها إلى العميل و الخادم.

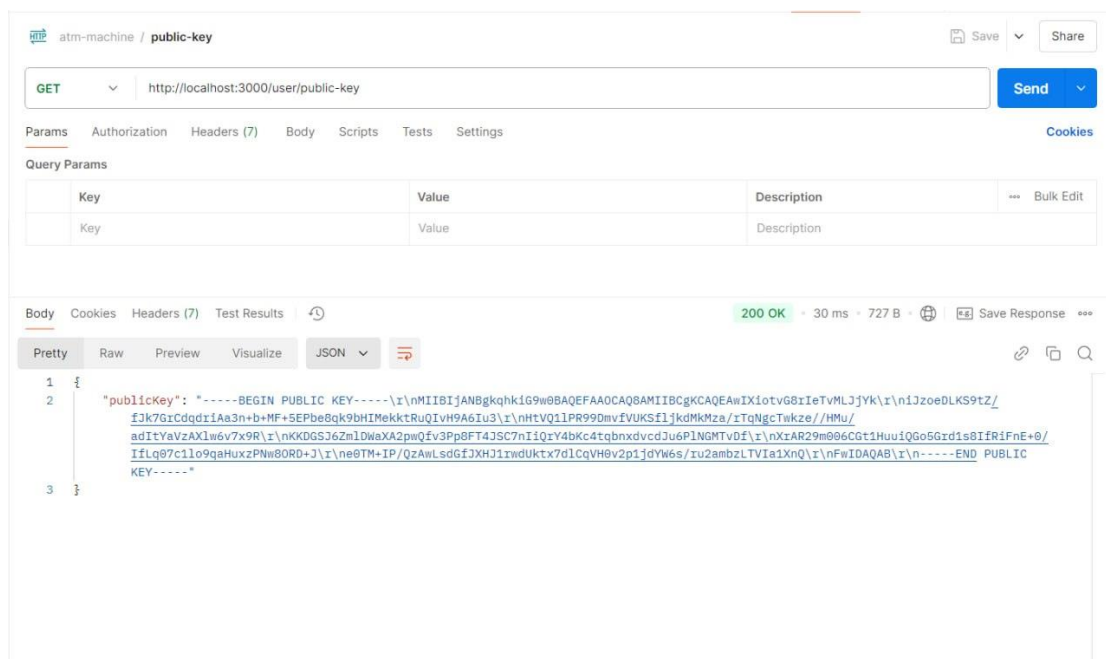
## 6. تصميم قاعدة البيانات

تتكون قاعدة البيانات من جدول واحد يسمى users مع الحقول التالية:

- id: المفتاح الأساسي
- username: معرف فريد للمستخدم
- encryptedPassword: كلمة المرور المشفرة باستخدام AES
- encryptedBalance: الرصيد المشفر باستخدام AES
- publicKey: المفتاح العام للمستخدم.

## 7. لقطات الشاشة وشرح كل مرحلة:

المرحلة 1: حصول المستخدم على المفتاح العام للسيرفر.



## المرحلة 2: تسجيل المستخدم

The screenshot shows a REST client interface for a service named 'atm-machine'. The request is a POST to 'http://localhost:3000/user/create'. The body is a JSON object with 'encUsername' and 'encPassword' fields. The response is a JSON object with 'message' and 'user' fields, indicating successful creation.

```
1 {
2   "encUsername": "Q66bZRXDUfrc4B8xj2PzPuCve1Z411zigMn0Mwz0hfk1NE9T2UUbFo
+PgXX9HripYZWYLKXpnn0lXRszT1QR6wc4IpEqYXPK4qD1U0FhnsKy0IPcQFr0CBZKEAo1SaL797AG5ypSMfuXHB4V8IISV1Xu8ooTSPw9eItNvk4pec/GK9zUd/
81v1P679ZK08XcL12mGuS0K+GNiUL7xx7W0YnpNY0iLZ97oEMxJjfb/Ygh0C87hLEMChAKN0RMq4362Z1cFvDPj1EGUvchcG6Vr2tZwHMyNpQs9KIwTgKI+37Fwtc
+9LzbuH0tJaybU0LKP8KQa8hMuEcdTTQ==",
3   "encPassword":
"iZC44nSASxV3iwpznvMLsbVMKZFvIhqwVV7E5Rq6Q4iRqRSJkrjQmuGhNEIOz2pfwva1BvdsVsT1253Wnh0YNI6WpZZJG85I7oZcEiYwPmFvDeoxw70AphFQEftb9usWZftMANP
/54YC90Ukpx1qzc/M/9Bd/Wlpo0BfjkVMffBK1bt6Tu1j1ZXMEJMOxukLMEC1G1Kx7fWYlM0Z/gX6+gAV9WZ2jGNT3TWv0omSIvcGwqaGv19W/
yB1J0tXfribUv0haBAMBIZuksBLx6S1rXUH517wNzc1+CISEYLPIDQu6/F+zbIfjh8NEi9tLn7dpQ8dSRaLkTLnprYKk6dmg==",
4   "publicKey": "-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwIX1otvG8RIeTVMLJjYk1JzoeDLKS9tZ/fjK7GrCdqdrifAa3n+b
+MF+5EPbe8q9bHIMekktRuQIvH9A6Iu3HTVQ11PR99DmvfVUKSf1jkdMkMza/iTqNgcTwkze//HMu/
adITaYvZAXlw6v7x9RKKDG536ZmLDwaXA2pwQfv3Pp8FT4J3JC7nIiQrY4bKc4tqbnxdvcdJu6PINGMTvDxiAR29m006CGt1Huu1Q6o5Gid1s8IfRiFnE+0/
IfLq07c11o9qaHuxzPNw80RD+Je0TM+IP/QzAwLsdGfjXH11wWUktx7d1CqVh0v2p1jdYw6s/ru2ambzLTVIa1XnQFwIDAQAB\n-----END PUBLIC KEY-----"
5 }
```

```
1 {
2   "message": "User created successfully",
3   "user": 7
4 }
```

\*الوصف\*: يمكن للمستخدمين التسجيل عن طريق إدخال اسم المستخدم وكلمة المرور الخاصة بهم المشفرين بواسطة المفتاح العام للسيرفر.

## المرحلة 3: تسجيل الدخول للمستخدم

The screenshot shows a REST client interface for a service named 'atm-machine'. The request is a POST to 'http://localhost:3000/user/login'. The body is a JSON object with 'encUsername' and 'encPassword' fields. The response is a JSON object with 'message' and 'user' fields, indicating successful login.

```
1 {
2   "encUsername": "akVj51/6UegA10fUs+TJ3ls6jMXpHedw0FxeZkdus6pJcjhpiDipEAM04C/p9YvuiB1Kn1LJL87tHF18hhZ0zntoZwI3IjgeYp8wKzw/aifankXPwTV0/qly/
z2f1tZs8SctnQCxsemb2ga4ts2B1tSP4TU0RfPiZVngXD1p/biLz5Yviy68/Mmv7TWfE06BNZK/
koITXEVAAnKwL7LT5YhmVoEsNSAQJXIGBoouAwtkkb2YRXQhmSM1reTaJQtn8Q9t5VdiMoCaGHjYg+7I86de
+iCoiTw67Zo8P0zbiXMODshj1LA0bnn3tsPMGidChsEKKVRmHLFDcnashCxxFg==",
3   "encPassword":
"iZC44nSASxV3iwpznvMLsbVMKZFvIhqwVV7E5Rq6Q4iRqRSJkrjQmuGhNEIOz2pfwva1BvdsVsT1253Wnh0YNI6WpZZJG85I7oZcEiYwPmFvDeoxw70AphFQEftb9usWZftMANP
/54YC90Ukpx1qzc/M/9Bd/Wlpo0BfjkVMffBK1bt6Tu1j1ZXMEJMOxukLMEC1G1Kx7fWYlM0Z/gX6+gAV9WZ2jGNT3TWv0omSIvcGwqaGv19W/
yB1J0tXfribUv0haBAMBIZuksBLx6S1rXUH517wNzc1+CISEYLPIDQu6/F+zbIfjh8NEi9tLn7dpQ8dSRaLkTLnprYKk6dmg==",
4   "publicKey": "-----BEGIN PUBLIC KEY-----\nMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMXsFwncABrEZ5sut+p8SkqqYQ3FyFvY\nn9A1SNS5VHEo2/SYC3AD/
T12Z1KF3JmJrtYVo0m4ecYU1ewT1cw6L+SECAwEAQ==\n-----END PUBLIC KEY-----"
5 }
```

```
1 {
2   "message": "Login successfully",
3   "user": 5
4 }
```

\*الوصف\*: يقوم المستخدمون بتسجيل الدخول باستخدام بيانات مشفرة من خلال المفتاح العام للسيرفر، والتي يتم نقلها بأمان إلى الخادم.

## المرحلة 3: عملية الإيداع

The screenshot shows a REST client interface for a 'Deposit' endpoint. The request is a POST to 'http://localhost:3000/user/deposit'. The body is a JSON object with 'userId' 15 and a large 'amount' string. The response status is '201 Created' with a body containing a 'balance' field and a large string value.

```
1 {
2   "userId": 15,
3   "amount": "n+EQSUXK2VLThh6FLxdYFIW7U/R3U/nXyTeGoncyjztv7BdIbfFk+BC9kqdBwxJ89/n8ZMz7w9MchexndRozIfG1WGMQtGvouWZX/
Mq9BhpFPcSYFtJrA84bnHfJnJLFZrJ8tpnpKex4qWgJkFntM1lpbdVem4x0J7w2khST5Hm71S2EImaT0fapFUmMYzkyf7Cy8gpffoo0kvI6dTaqBg/tt2CLDL4+h3SuyE0GZk8e/
uuWm9v1R5S40kQGwd4oiNaLXGsyAAPxF99FLuVJsgkCqOvf3p6vI13uJ0ae1ZidMYQV/ImwTUokihwP/NddTB+zReBqRzErmSc6w=="
4 }
```

```
1 {
2   "balance": "vf51xZHAqdAtm1omu05GKrn469UzW1lGy14onxVXD0GMF1WKR0KPNwEIQ0wm3Jcm4d4yYaRqV0b/
mMASyGRtUv8KfVGdcojHW0XyTrkjb81R19fDSVB6NDgogAgFjZD3CWKU4ENj7sa7JFw4TpjQJh2W1D3/U7Tqw05y2Eks6LqtVG6wNcr/MjSy0LYhM2zc4U7TIQkizKKU
+0CfZnbnNfeMNKn65FYv8VmYYXu7nbeTveHR6Awn86IVatD82xXQ6rUCt9xFK9pLBKfyFAk4tuELm/HcXrJhQ7Xoe6Ww1u193kyjR6a/dhFXSp2kRa44dcHv0P2ddPw+2wH
+WmZLzW=="
3 }
```

\*الوصف\*: يمكن للمستخدمين إيداع الأموال، والتي تتم معالجتها بأمان على الخادم.

## المرحلة 4: عملية السحب

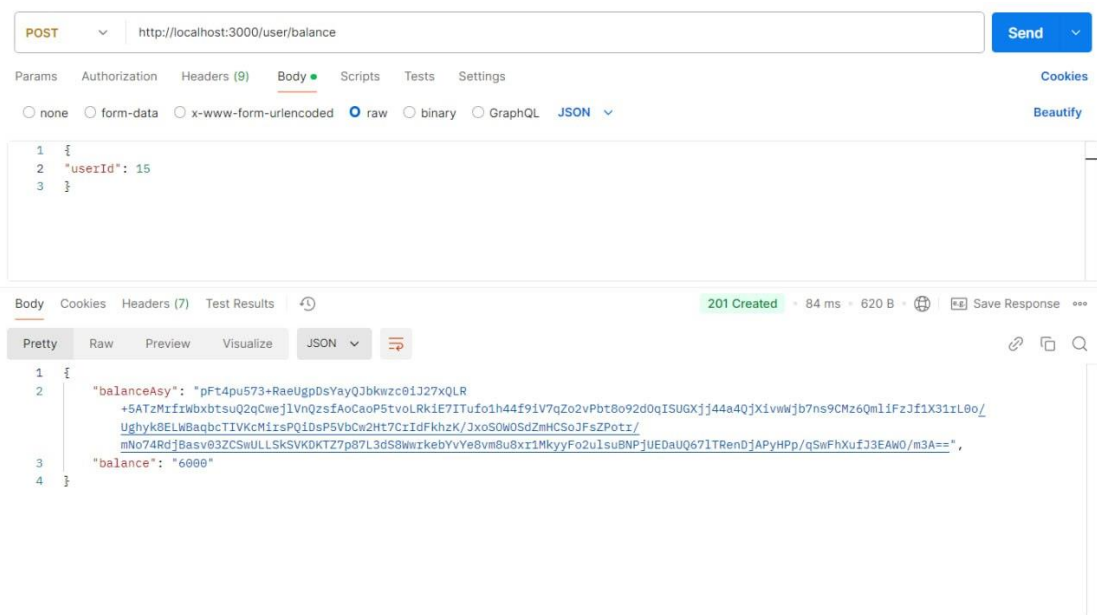
The screenshot shows a REST client interface for a 'Withdraw' endpoint. The request is a POST to 'http://localhost:3000/user/withdraw'. The body is a JSON object with 'userId' 15 and a large 'amount' string. The response status is '201 Created' with a body containing a 'message' field with the value 'Withdrawal successful'.

```
1 {
2   "userId": 15,
3   "amount": "n+EQSUXK2VLThh6FLxdYFIW7U/R3U/nXyTeGoncyjztv7BdIbfFk+BC9kqdBwxJ89/n8ZMz7w9MchexndRozIfG1WGMQtGvouWZX/
Mq9BhpFPcSYFtJrA84bnHfJnJLFZrJ8tpnpKex4qWgJkFntM1lpbdVem4x0J7w2khST5Hm71S2EImaT0fapFUmMYzkyf7Cy8gpffoo0kvI6dTaqBg/tt2CLDL4+h3SuyE0GZk8e/
uuWm9v1R5S40kQGwd4oiNaLXGsyAAPxF99FLuVJsgkCqOvf3p6vI13uJ0ae1ZidMYQV/ImwTUokihwP/NddTB+zReBqRzErmSc6w=="
4 }
```

```
1 {
2   "message": "Withdrawal successful"
3 }
```

\*الوصف\*: يمكن للمستخدمين سحب الأموال بعد التحقق من وجود رصيد كافٍ.

## المرحلة 5: التحقق من الرصيد



\*الوصف\*: يمكن للمستخدمين التحقق من رصيدهم بشكل آمن

## 8. الخاتمة

تطبيق محاكاة الصراف الآلي يوضح بنجاح كيفية التعامل بشكل آمن مع المعاملات المالية الحساسة من خلال استخدام تقنيات التشفير المتقدمة. من خلال استخدام خوارزمية RSA للتواصل الآمن و AES لتخزين البيانات، نضمن أن تظل معلومات المستخدمين سرية ومحفوظة ضد الوصول غير المصرح به. لا يقتصر هذا المشروع على تلبية متطلبات الوظائف المحددة. فحسب، بل يتماشى أيضاً مع أفضل الممارسات في أمان البرمجيات.