جامعة دمشق
كلية الهندسة المعلوماتية
قسم هندسة البرمجيات

cryptocurrency

تقرير أمن المعلومات

إعداد الطلاب:

آلاء الحموي

محمد باسل الشمالي

محمد غانم

هانئة المالكي

توصيف المشروع:

المشروع عبارة عن مجموعة برنامج مكتوبة بلغة C#، تتخاطب فيما بينها بيانات باستخدام بروتكول TCP/IP بحيث أنها تمثل نظام عملة إلكترونية مبسط، والبرامج هي:

البرنامج الأول Server: وهو الذي يمثل المخدم الرئيسي ويحوي على قاعدة البيانات العملاء وهو الذي يجري عمليات التحويل بين حسابات العملاء.

البرنامج الثاني Client: وهو البرنامج الذي يستخدمه العميل ويقدم مجموعة من الوظائف وهي:

- تسجيل الدخول والخروج.
- تسجيل حساب جديد.
- التحقق من الرصيد الحالي.
- تحويل إلى رصيد عميل آخر.

البرنامج الثالث Certification Authority: هو يمثل جهة ثالثة موثقة لدى الطرفين حيث يقوم العميل بطلب شهادة الكترونية من هذا البرنامج و يقوم المخدم بالتأكد من صحة هذه الشهادة.

آلية عمل النظام:

يبتدئ النظام كما هو مطلوب بمجموعة من العملاء ولكل عميل رصيد معين، المخدم دوماً في حالة عمل وينتظر الطلبات من برامج العملاء لمعالجتها.

تسجيل الدخول:

يستقبل المخدم المعلومات من العميل وهي في مشروعنا اسم مستخدم وكلمة سر ويقوم بالتحقق منها، ففي حال كانت المعلومات صحيحة يمكن للعميل متابعة باقي الوظائف (التحقق من الرصيد والتحويل) وإلا يرسل المخدم رسالة خطأ تعبر عن نوع الخطأ الحاصل (لا يوجد عميل لهذا الاسم، كلمة السر خاطئة، ... الخ).

تسجيل حساب جديد:

يستقبل المخدم المعلومات من العميل وهي في مشروعنا الاسم واسم المستخدم وكلمة السر ويقوم بالتحقق منها، ففي حال كان اسم المستخدم غير موجود مسبقاً يقوم بأنشاء حساب جديد لهذا العميل وتكون القيمة الابتدائية لرصيده هي صفر، وإلا يرسل المخدم رسالة خطأ للعميل تخبره بأن اسم المستخدم تم استخدامه من قبل.

التحقق من الرصيد الحالي للعملاء:

بعد أن يكون العميل قد سجل دخوله بالمعلومات الصحيحة يرسل العميل إلى المخدم طلب الحصول على الرصيد الحالي للعملاء ، المخدم يستقبل الطلب ويعالجه ويعيد قيمة الرصيد الموافق لِلعملاء الحاليين للنظام.

التحويل إلى رصيد آخر:

بعد أن يكون العميل قد سجل دخوله بالمعلومات الصحيحة يرسل العميل إلى المخدم طلب تحويل بحيث يحوي على ID العميل الذي يريد تحويل له وكمية المال الذي يريد تحوليه، المخدم يستقبل الطلب ويعالجه ويعيد نتيجة التحويل إما النجاح أو الفشل.

المتطلبات الأمنية للنظام:

بحسب ما سبق انتقال المعلومات السابقة عبر شبكة مفتوحة مثل الانترنيت له العديد من المشاكل الأمنية:

- يمكن لأي برنامج اعتراض المعلومات المرسلة من العميل ورؤيتها => نحتاج إلى خصوصية Privacy.
- يمكن لأي برنامج توليد بعض المعلومات المرسلة وإرسالها على أنه عميل حقيقي => نحتاج إلى مصادقة المستخدمين Authentication.
- يمكن لأي عميل نكران عملية التحويل => نحتاج إلى آلية لتنفيذ عدم النكران Non-Repudiation.
- يمكن لأي برنامج اعتراض ثم تعديل المعلومات المرسلة => نحتاج إلى اتساق ووحدة البيانات Integrity.

تحقيق المتطلبات الأمنية:

1. تنفيذ عملية الاستعلام مع الحفاظ على خصوصية العملاء:

تم استخدام خوارزمية التشفير المتناظر AES كما هو وارد في نص المشروع.

خطوات العمل:

الخطوات التالية توضح آلية الاستعلام عن الرصيد الحالي للعملاء:

- عندما يبدأ برنامج العميل بالعمل يحاول الاتصال بالمخدم ففي حال نجحت عملية الاتصال يقوم المخدم بإرسال مفتاح عام وهذا المفتاح قد تم توليده سابقاً عندما بدء المخدم بعمله.
- بعد أن يتأكد المخدم من عضوية العميل يقوم بإرسال مفتاح التشفير لخوارزمية AES و من أجل الحفاظ على خصوصية العملاء و منع المستخدمين من خارج النظام من الحصول على المفتاح يتم تشفير المفتاح باستخدام المفتاح العام للعميل الذي أثبت عضويته.
- يستقبل العميل المفتاح المتناظر مشفراً و يقوم بفك تشفيره من خلال المفتاح الخاص للعميل ويحتفظ به، عندما يريد العميل التحقق من الرصيد الحالي يقوم العميل بإرسال طلب إلى المخدم وبما أنه لا يحوي أي معلومات فلا يوجد أي عملية تشفير.
- يقوم المخدم باستقباله ومعالجته باستعلام على قاعدة البيانات للحصول على معلومات العملاء الموجودين بالنظام، يقوم المخدم بمعالجة معلومات العملاء بحيث تصبح عبارة عن قيمة نصية واحدة كل عميل مع قيمة رصيده، ولكي نحافظ على خصوصية العملاء يجب تشفير هذه القيمة النصية باستخدام المفتاح المتناظر لخوارزمية AES الذي أصبح متوفراً لدى المخدم و العميل.
- يرسل المخدم القيمة المشفرة إلى العميل.
- يستقبل العميل القيمة المشفرة ويقوم بفك تشفيرها باستخدام مفتاح AES الذي تم الحصول عليه سابقاً.
- بعد فك التشفير يقوم برنامج العميل بعرض نتيجة الطلب وهي قائمة فيها اسم كل عميل وقيمة رصيده.

2. تنفيذ عملية التحويل باستخدام RSA

خطوات العمل:

الخطوات التالية توضح آلية التحويل:

- عندما يبدأ برنامج العميل بالعمل يحاول الاتصال بالمخدم ففي حال نجحت عملية الاتصال يقوم المخدم بإرسال مفتاحه عام وهذا المفتاح قد تم توليده سابقاً عندما بدء المخدم بعمله.
- يستقبل العميل المفتاح العام ويحتفظ به، عندما يريد العميل إجراء عملية التحويل يقوم بإرسال طلب إلى المخدم بحيث يحوي هذا الطلب على ID العميل المرسل وID العميل المستقبل وكمية المال المحول Amount، ويجب تشفير هذا الطلب وما يحوي من معلومات ويتم تشفيره باستخدام المفتاح العام للمخدم الذي تم استقباله سابقاً.
- بعد عملية التشفير يرسل الطلب إلى المخدم.
- يقوم المخدم باستقبال الطلب المشفر ليقوم بفك تشفيره باستخدام المفتاح الخاص به، وبعد الحصول على القيم الثالثة السابقة يقوم المخدم بإجراء عمليات التحقق من قيمة التحويل موجبة أم سالبة والتحقق من وجود المستخدمين المرسل والمستقبل وفي حال نجحت عمليات التحقق يرسل المخدم رسالة تأكيد إلى برنامج العميل تخبره بنجاح عملية التحويل.

3. تنفيذ عملية التحويل باستخدام PGP

خطوات العمل:

الخطوات التالية توضح آلية التحويل مع تحقيق مبدأ عدم النكران باستخدام التوقيع الالكتروني:

- عندما يبدأ برنامج العميل بالعمل يحاول الاتصال بالمخدم ففي حال نجحت عملية الاتصال يقوم المخدم بإرسال مفتاحه عام وهذا المفتاح قد تم توليده سابقاً عندما بدء المخدم بعمله، كما يقوم العميل بتوليد مفتاح بشكل عشوائي يسمى Session Key.
- يستقبل العميل المفتاح العام ويحتفظ به، عندما يريد العميل إجراء عملية التحويل يقوم بإرسال طلب إلى المخدم بحيث يحوي هذا الطلب على ID العميل المرسل وID العميل المستقبل وكمية المال المحول Amount، ويجب تشفير هذا الطلب وما يحوي من معلومات ويتم تشفيره باستخدام المفتاح السابق Session Key، كما يقوم برنامج العميل بتشفير المفتاح السابق SK باستخدام المفتاح العام الذي استلمه من المخدم.
- بعد انتهاء عملية التشفير يتولد لدينا قيمة X، يقوم برنامج المخدم بتطبيق تابع هاش على القيمة X ليقوم بعدها بتشفير قيمة تابع الهاش باستخدام مفتاحه الخاص فينتج القيمة Y.
- يقوم برنامج العميل بأرسال القمتين X و Y إلى المخدم.
- يقوم المخدم باستقبال القيمتين السبقتين X و Y المشفرتين ليقوم بتطبيق نفس تابع الهاش على القيمة X ويطابقها مع القيمة الناتجة عن فك تشفير القيمة Y باستخدام المفتاح العام للعميل المرسل وفي حال التطابق نستنتج أن القيمة المستقبلة فعلاً من هذا العميل وأن القيمة لم يتم تعديلها.
- القيمة X تمثيل قيمتين هما تشفير SK وتشفير لمعلومات التحويل، يقوم المخدم بفك تشفير SK باستخدام المفتاح الخاص لديه، ثم يقوم باستخدام SK لفك تشفير معلومات التحويل، وبعد الحصول على القيم الثالثة السابقة يقوم المخدم بإجراء عمليات التحقق من قيمة التحويل موجبة أم سالبة والتحقق من وجود المستخدمين المرسل والمستقبل وفي حال نجحت عمليات التحقق يرسل المخدم رسالة تأكيد إلى برنامج العميل تخبره بنجاح عملية التحويل.

4. التحقق من صحة العضوية :

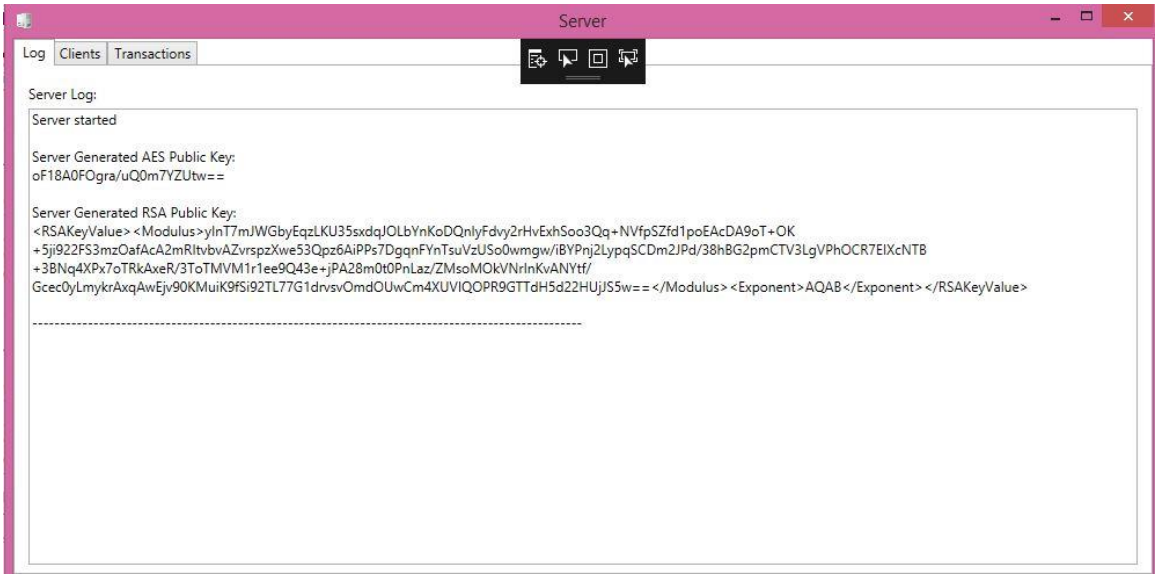
خطوات العمل:

تتم عملية التحقق من خلال الخطوات التالية:

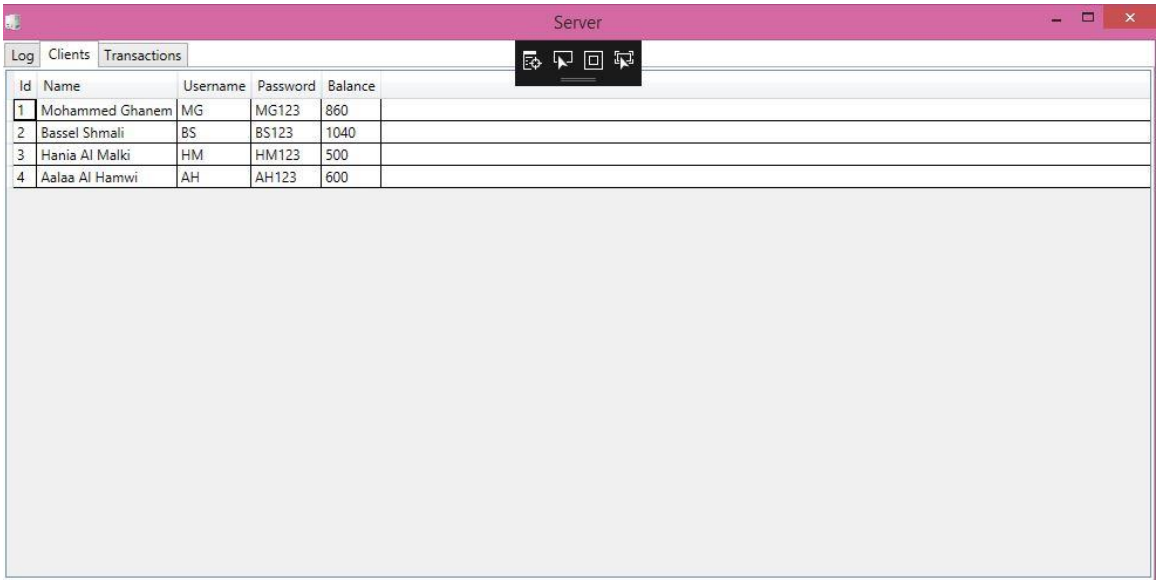
1. عندما يقوم العميل بطلب تسجيل حساب يقوم البرنامج أولا بإرسال طلب إلى Certification Authority لطلب شهادة الكترونية يرسل بالطلب اسم العميل و المفتاح العام له.
2. في حالة عدم موافقة Certification Authority على إصدار شهادة حيث تتم الموافقة بشكل يدوي يتم إرسال رسالة خطأ إلى العميل و لا يتمكن من متابعة تسجيل حساب.
3. في حالة الموافقة ترسل الشهادة إلى العميل حيث تحوي معلومات مثل اسم العميل و المفتاح العام التابع له و رقم تسلسلي و تاريخ الإصدار و الجهة التي قامت بتصديق الشهادة و توقيع هذه الجهة.
4. لكي يتابع عملية تسجيل حساب يقوم العميل بإرسال الشهادة إلى المخدم الذي بدوره يتحقق من صحتها من خلال المفتاح العام للـ Certification Authority .
5. في حالة التأكد من صحة الشهادة يقوم العميل بتشفير بيانات تسجيل حساب من خلال المفتاح العام للمخدم.
6. يقوم المخدم بالتأكد من صلاحية البيانات و يرسل رد إما نجاح أوفشل.
7. إذا تم تسجيل الحساب بنجاح يقوم المخدم بتشفير مفتاح خوارزمية AES بالمفتاح العام للمخدم.
8. يقوم المخدم بفك تشفير المفتاح و الاحتفاظ به من أجل فك تشفير نتائج الاستعلام عن رصيد من المخدم.

التنفيذ :

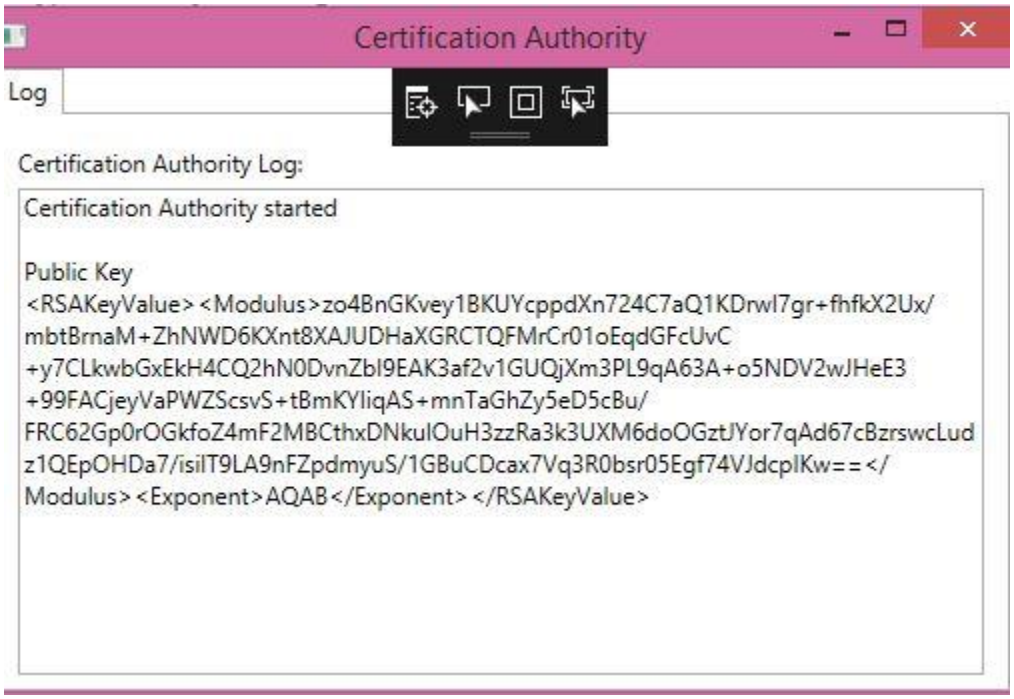
أولا يبدأ المخدم العمل حيث يولد المفتاح العام و المف تاح المتناظر لـAES:



يبدأ المخدم بمجموعة من العملاء الموجودين سابقاً:

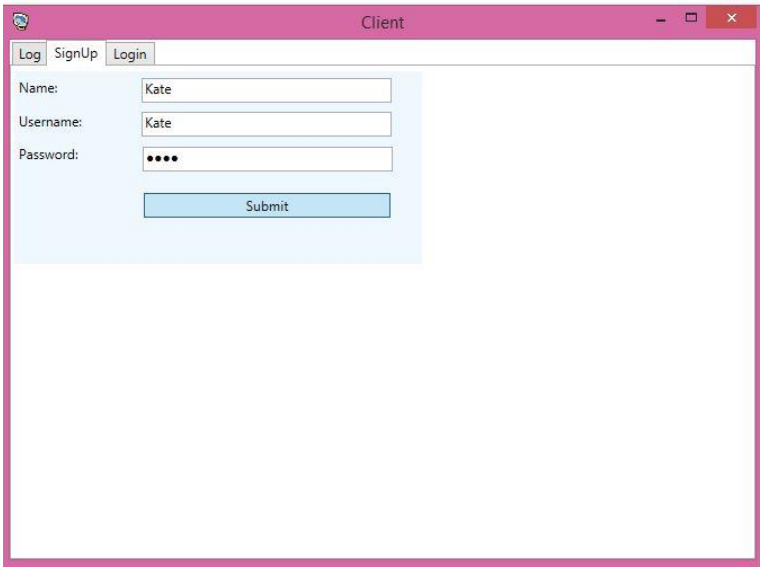


يبدأ برنامج Certification Authority و يولد المفتاح العام الخاص

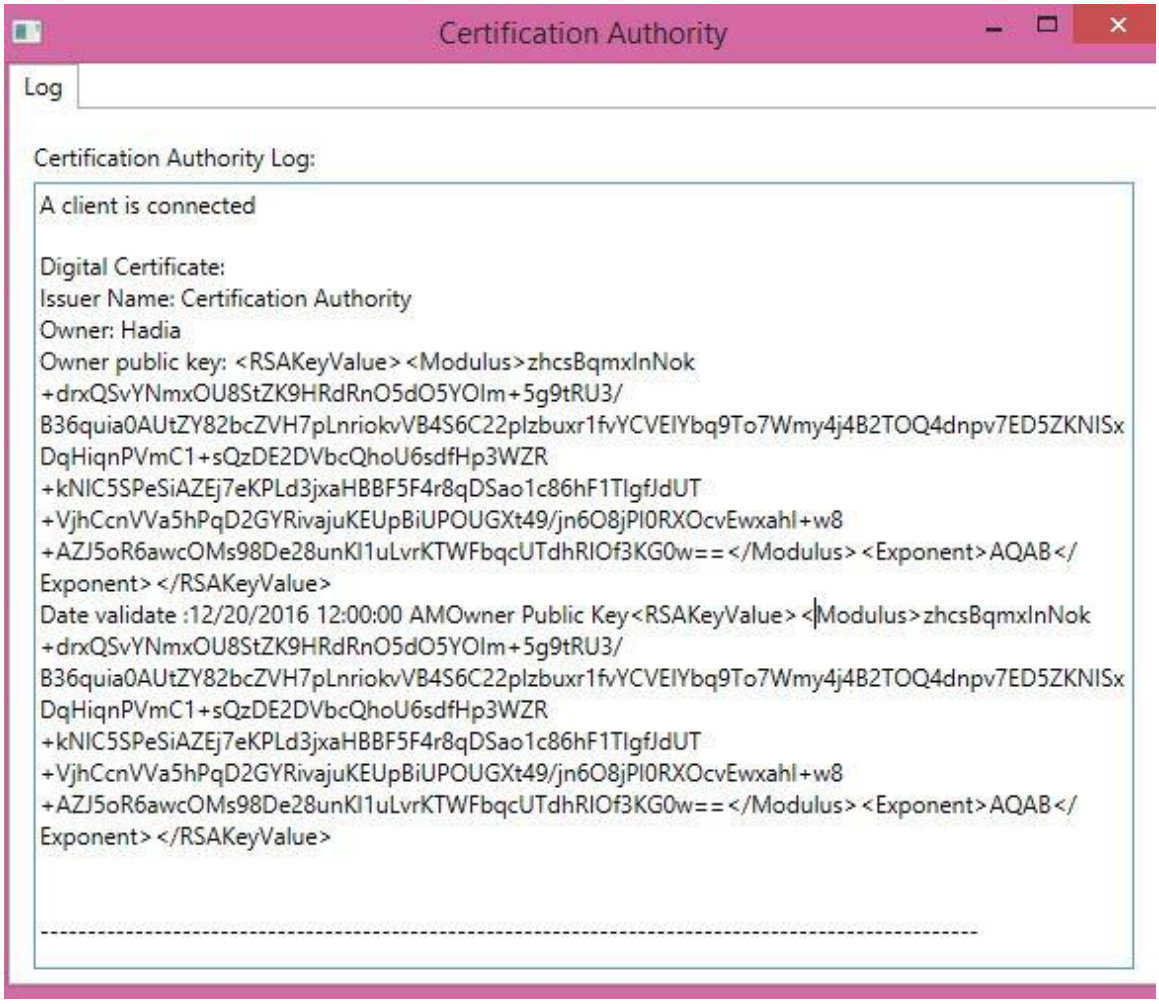


يبدأ برنامج العميل نختار تسجيل حساب جديد:

عند الضغط على زر submit يقوم بإرسال طلب من أجل الحصول على شهادة الكترونية



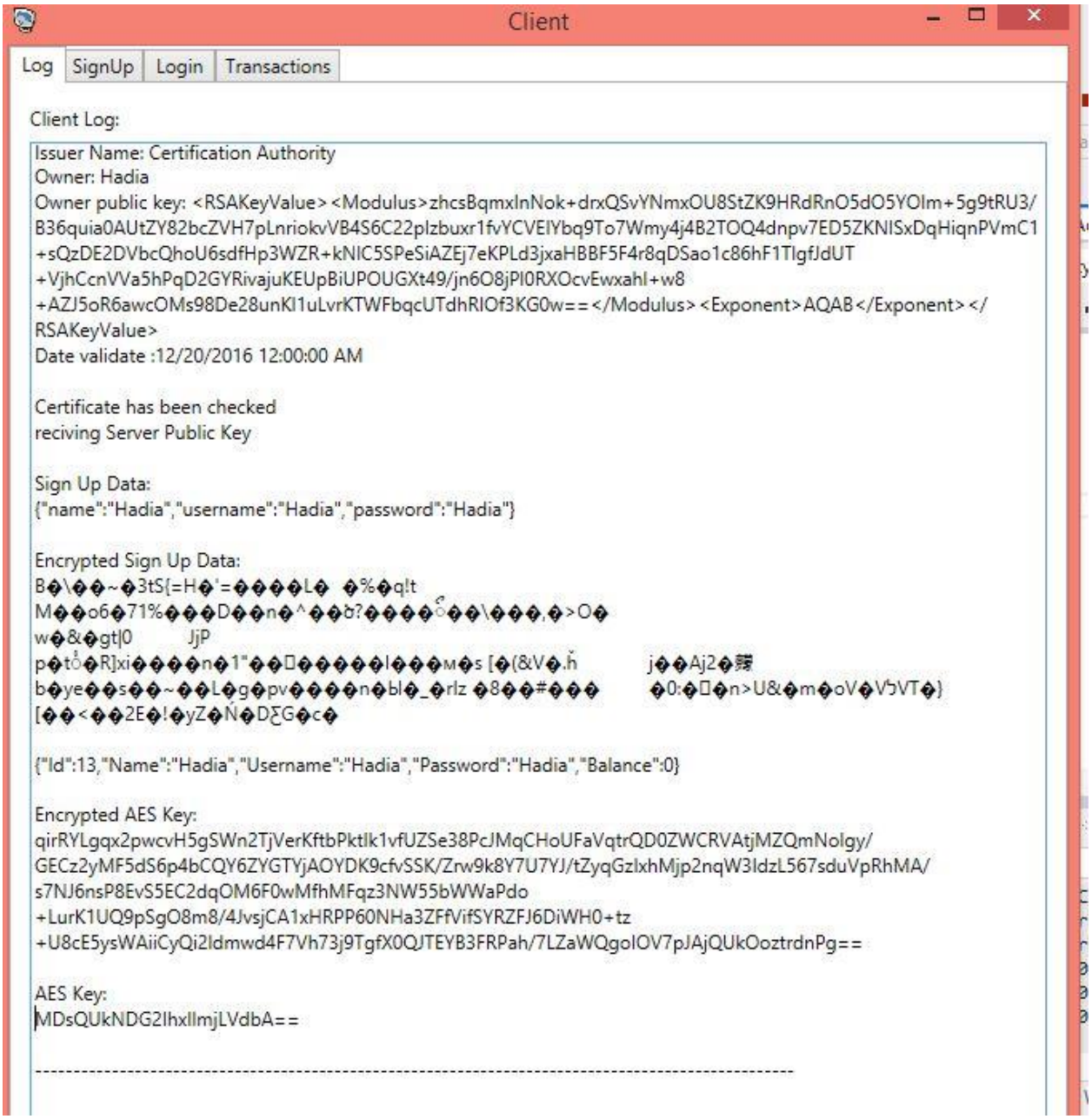
عندما يصل الطلب إلى Certification Authority تقوم بتوليد الشهادة الالكترونية و التوقيع عليها



ثم تظهر رسالة للموافقة على الشهادة أو الرفض

في حال الموافقة ترسل الشهادة إلى العميل الذي يقوم بدوره بإرسالها إلى المخدم حيث يتأكد المخدم من صحة الشهادة و في حال كان صحيحة يرسل العميل بيانات التسجيل مشفرة بالمفتاح العام للمخدم الذي يقوم بدوره بفك التشفير بمفتاحه الخاص و في حال كانت البيانات صالحة يقوم المخدم بإنشاء حساب و إرسال المفتاح المتناظر AES مشفرا بمفتاح العميل العام الموجود بالشهادة و يحتفظ به العميل لاستخدامه فيما بعد :

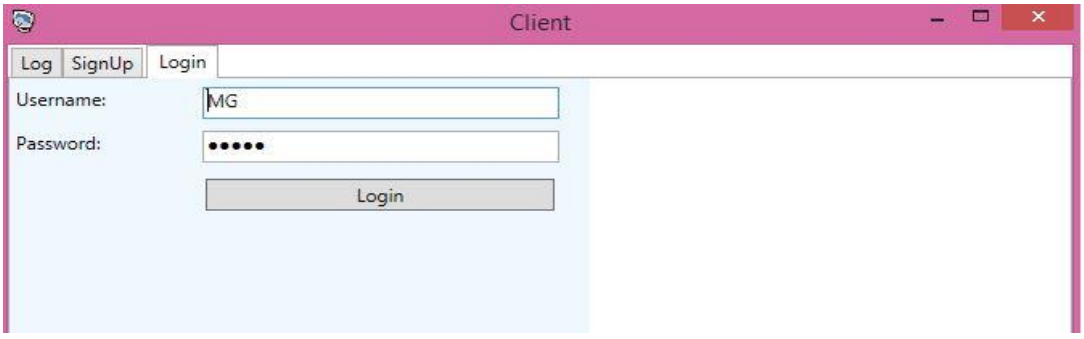
نافذة العميل و تحوي الشهادة و معلومات التسجيل قبل و بعد التشفير



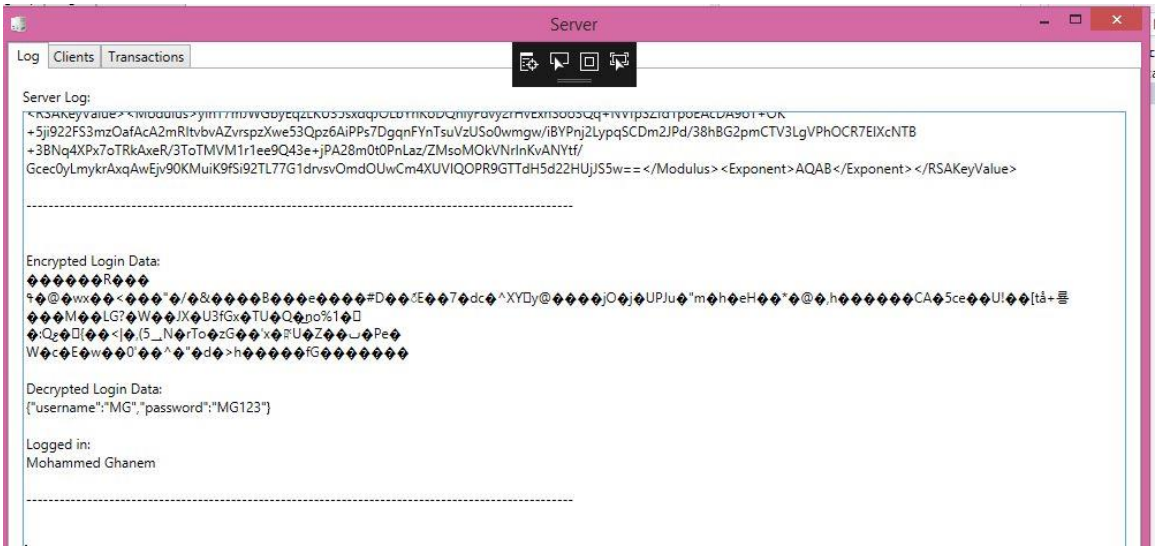
نافذة المخدم

إضافة العميل إلى قاعدة بيانات المخدم

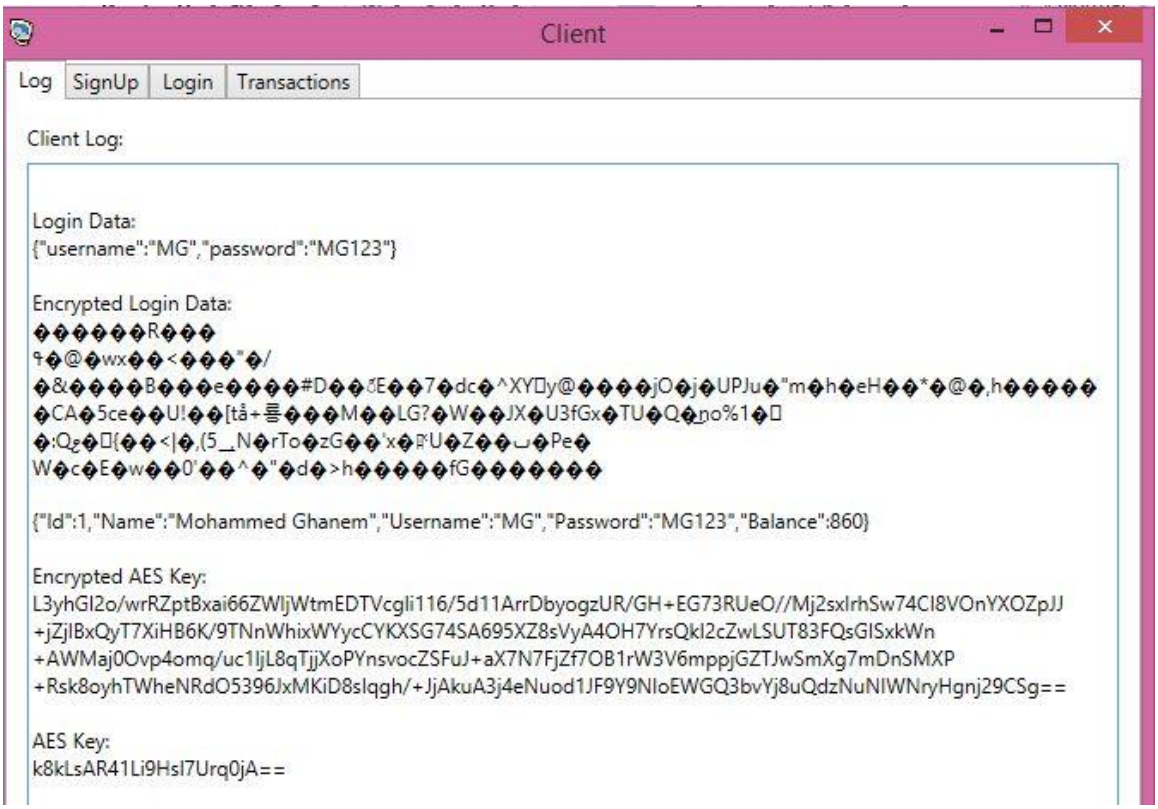
في حال كان تسجيل الدخول عن طريق حساب سابق مما يعني أن المخدم سبق و تأكد من عضوية هذا العميل لذلك بعد أن يدخل بيانات الحساب صحيح يقوم المخدم بتشفير المفتاح المتناظر بالمفتاح العام للعميل و يقوم العميل بفك التشفير بمفتاحه الخاص من أجل استخدام هذا المفتاح في الاستعلام عن رصيد باقي العملاء:



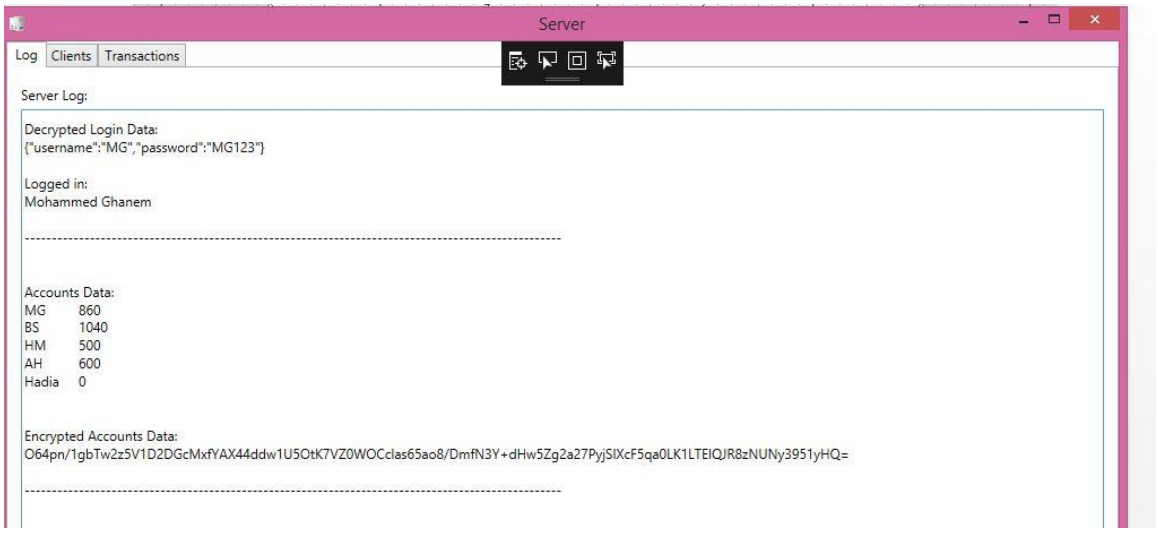
نافذة المخدم



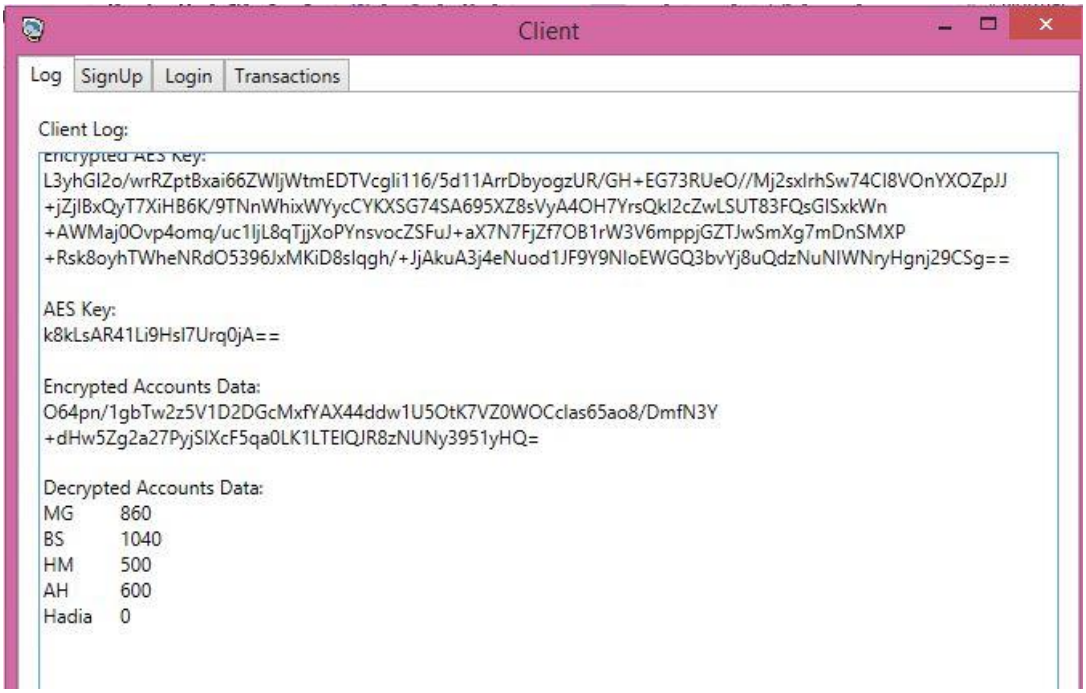
نافذة العميل



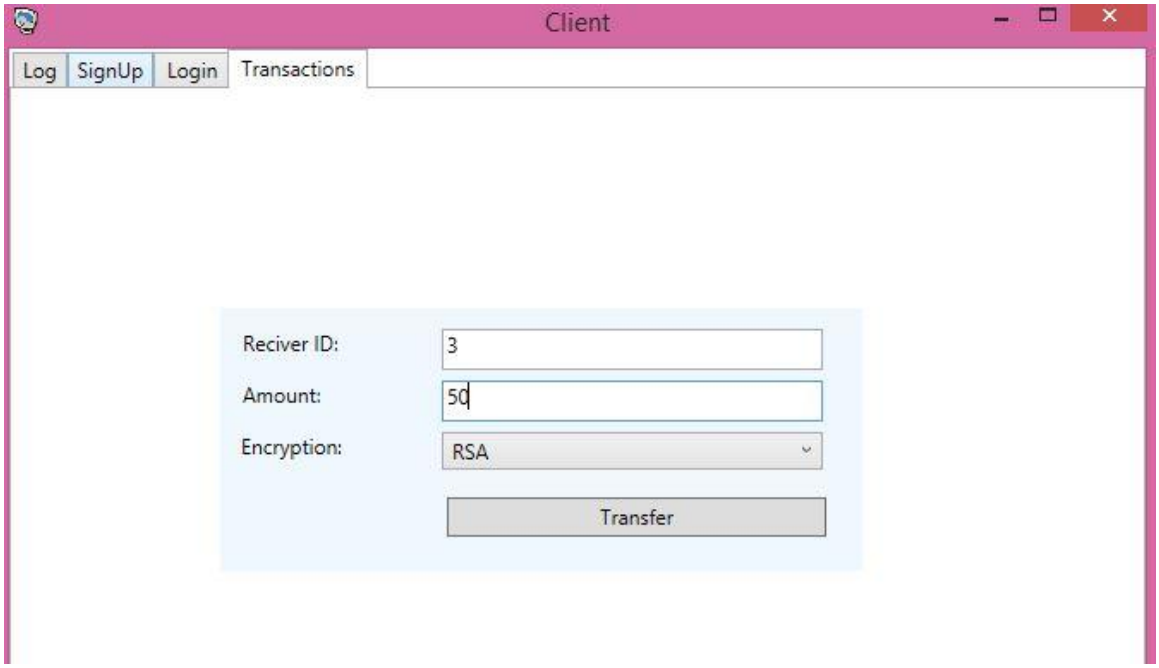
بعد تسجيل الدخول أصبح بإمكان العميل الاستعلام عن القيمة المالية الحالية للعملاء يقوم بإرسال طلب إلى المخدم الذي ينشئ قائمة تحوي على أسماء العملاء و القيمة المالية التي يمتلكها كل عميل و يقوم بتشفير هذه القائمة باستخدام خوارزمية AES:



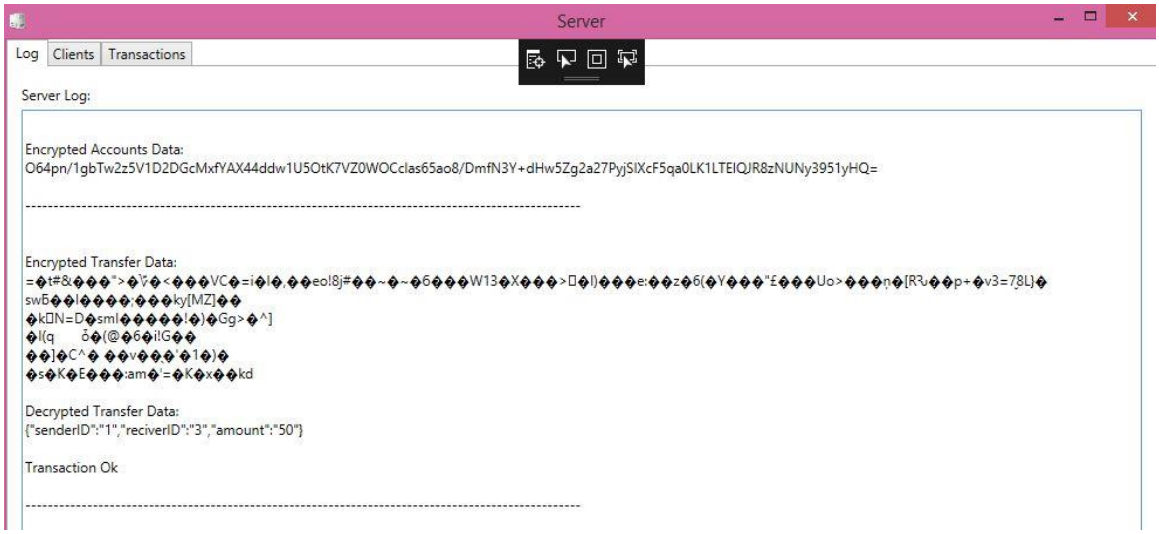
يقوم العميل باستقبال البيانات المشفرة و فك تشفيرها باستخدام المفتاح المتناظر و خوارزمية AES:



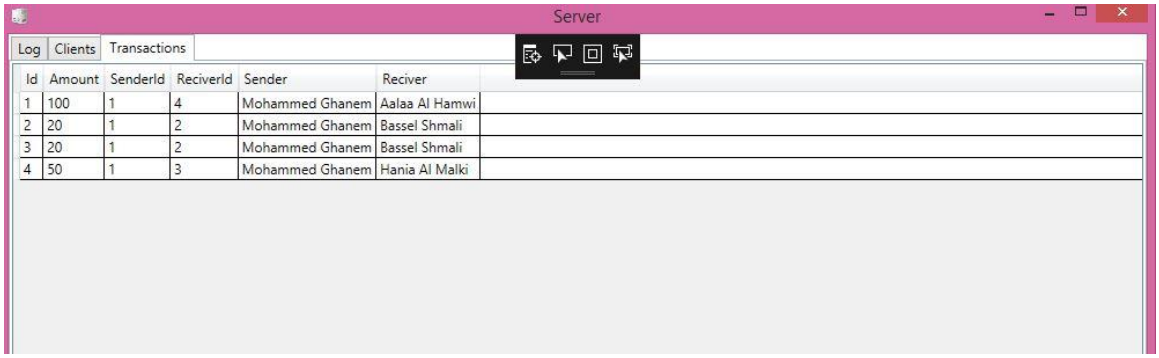
يستطيع العميل أيضا أن يقوم بمناقلة و يحدد خوارزمية التشفير التي يريد استخدامها لتشفير البيانات بعد أن يحدد id المرسل إليه و المبلغ :



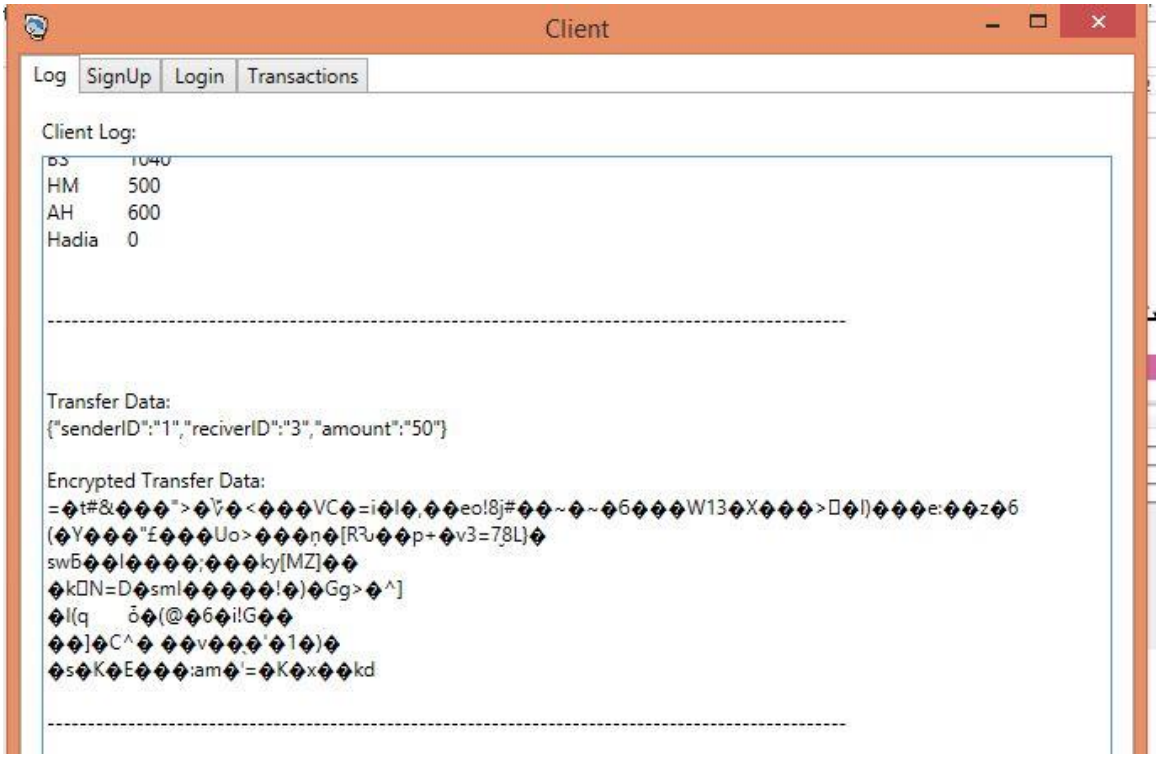
ترسل البيانات مشفرة بخوارزمية RSA إلى المخدم الذي يقوم بفك تشفيرها و التأكد من تحقق شروط عملية المناقلة ثم يسجل المناقلة في سجل المناقلات و يرسل إلى المخدم أن العملية تمت بنجاح



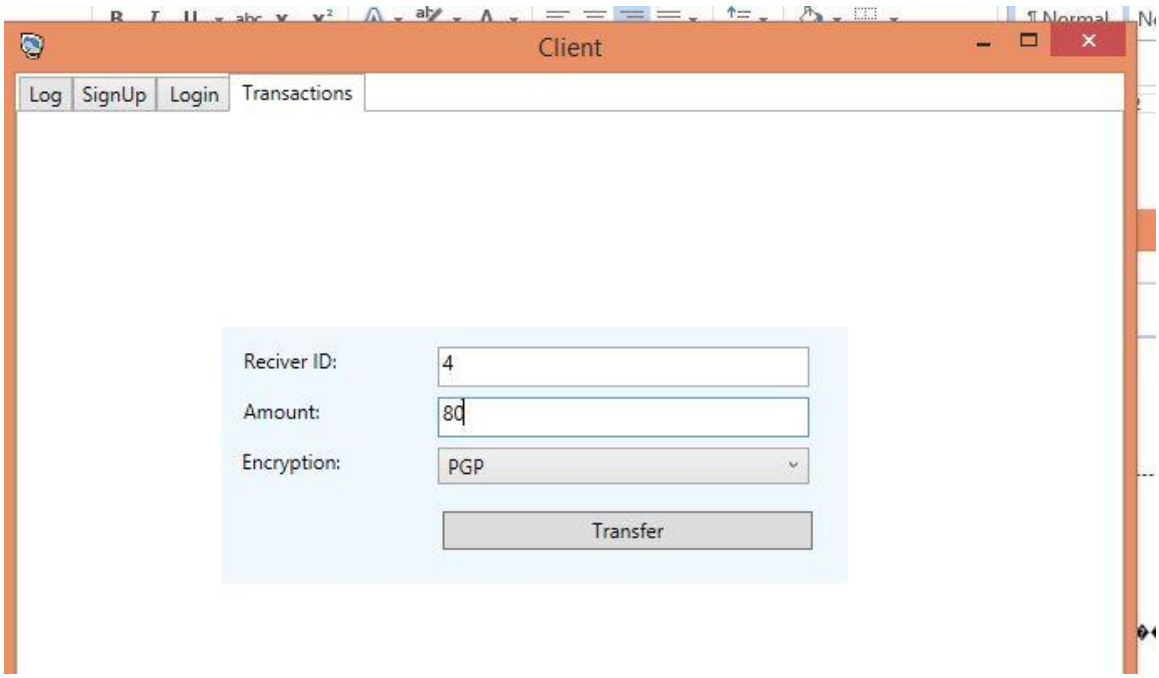
إضافة المناقلة إلى قاعدة المعطيات :



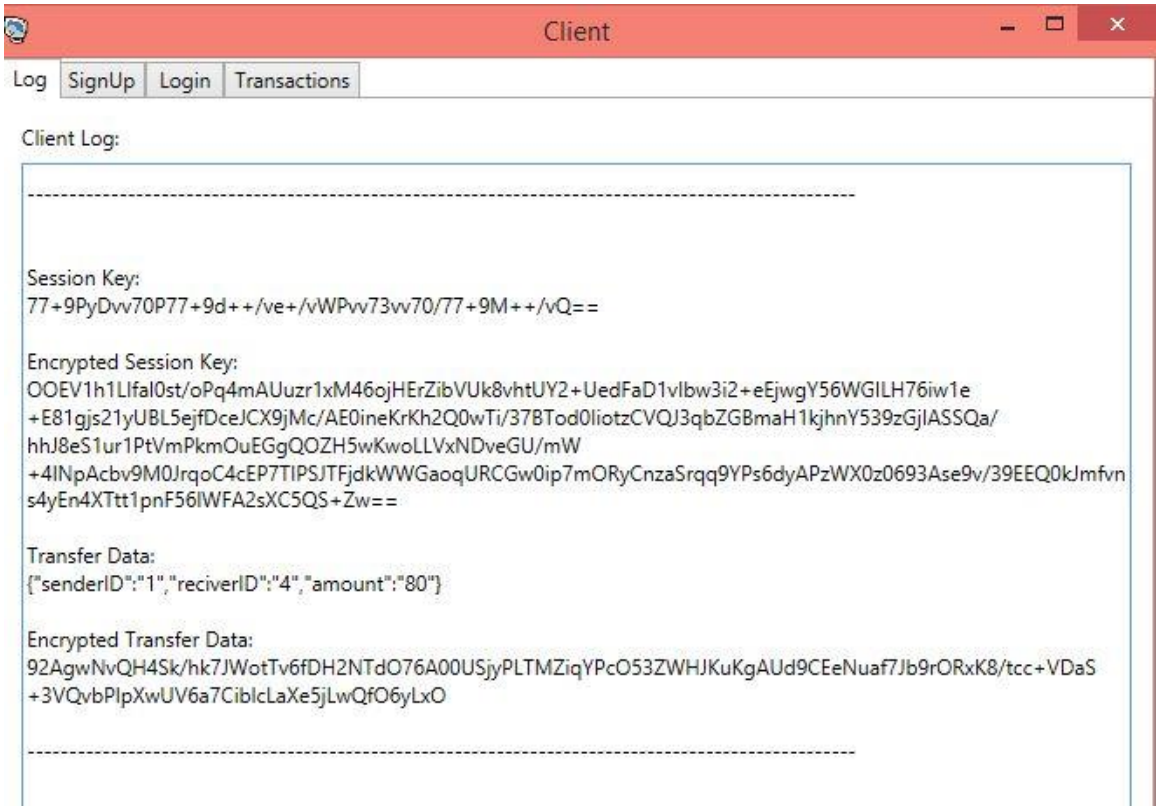
نافذة العميل :



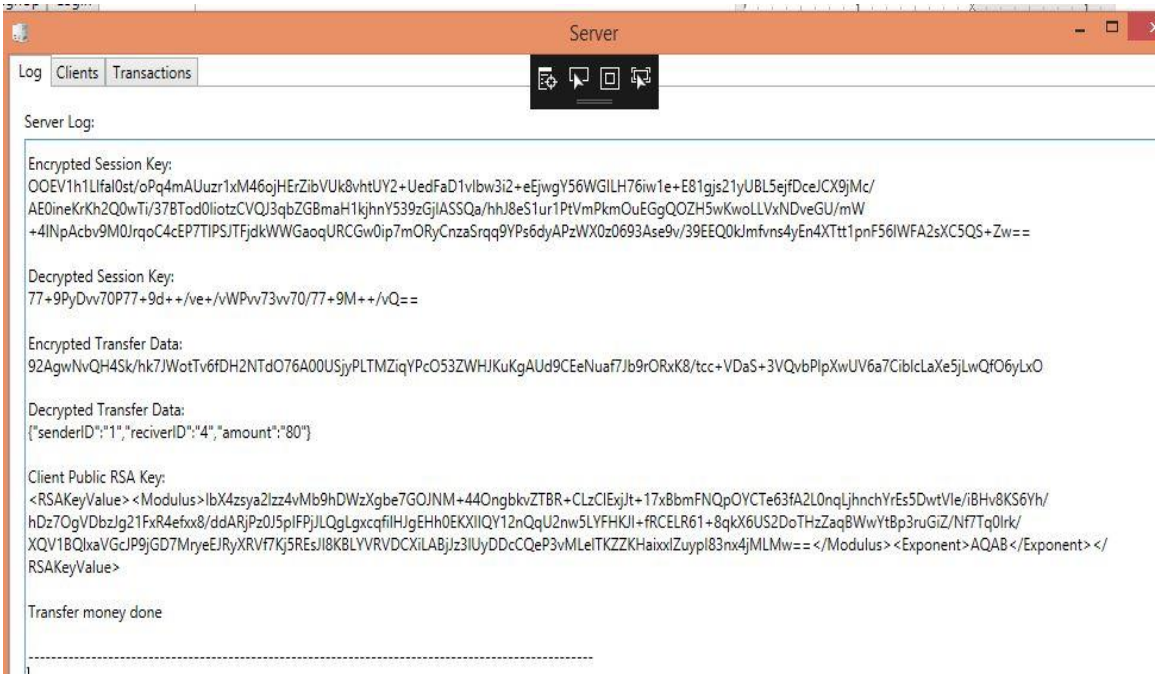
تنفيذ المناقلة باستخدام PGP:



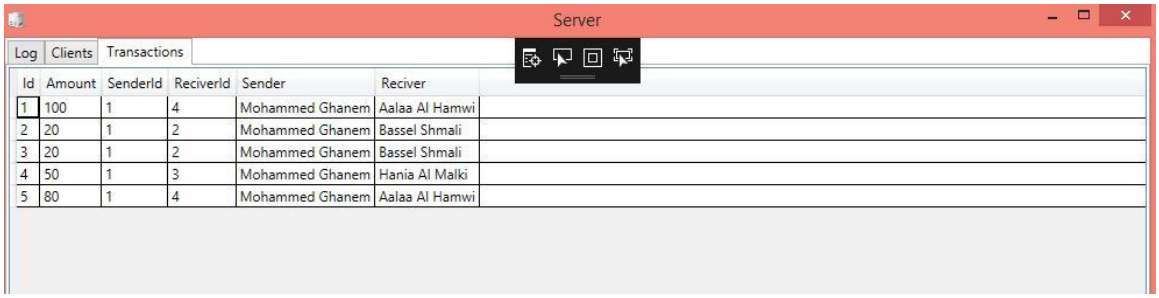
يقوم العميل بتوليد session key و تشفيره و إرساله إلى المخدم ثم إرسال بيانات المناقلة مشفرة بمفتاح session key



واجهة المخدم



إضافة المناقلة إلى قاعدة المعطيات :



Id	Amount	SenderId	ReciverId	Sender	Reciver
1	100	1	4	Mohammed Ghanem	Aalaa Al Hamwi
2	20	1	2	Mohammed Ghanem	Bassel Shmali
3	20	1	2	Mohammed Ghanem	Bassel Shmali
4	50	1	3	Mohammed Ghanem	Hania Al Malki
5	80	1	4	Mohammed Ghanem	Aalaa Al Hamwi