كلية الهندسة المعلوماتية

السنة الخامسة
عملي أمن نظم المعلومات

نظام عملة إلكترونية مبسط

نظام عملة إلكترونية قائم على التشفير cryptocurrency مبسط يسمح بتحويل الأموال بين مجموعة من العملاء الذي يتواصلون عبر شبكة مفتوحة مثل شبكة الإنترنت.

يتضمن النظام مخدم server تتضمن سجل مركزي بجميع عمليات التبادل transactions التي تمت بين جميع العملاء clients ، وسجل آخر يتضمن سجل خاص بكل عميل ويعكس القيمة المالية الحالية التي يمتلكها هذا العميل.

يعمل النظام وفق القواعد التالية التي يمكن من خلالها استنتاج المتطلبات الأمنية للنظام:

- يبتدئ النظام بمجموعة من القيم المالية الأولية لكل عميل التي يجب أن يظل مجموعها ثابتا مع مرور الزمن، يتم تعريف كل عضو بعنوان IP أو اسم نطاق domain خاص.
- يمكن في أي لحظة لأي عميل أن يستعلم عن القيمة المالية الحالية للعملاء الآخرين الموجودين في النظام من المخدم المركزي، ويجب عدم السماح لأي جهة خارج النظام من الاطلاع على أي من المعلومات المالية للعملاء، ويتم تنظيم هذا من خلال مفتاح سري مشارك بين الأعضاء.
- تتم عملية التحويل عندما يقوم أحد العملاء بإنشاء غرض transaction يتضمن اسم المرسل، واسم المرسل إليه، وقيمة التحويل (قيمة موجبة)، ويرسل هذا الغرض إلى المخدم المركزي، ثم يقوم المخدم المركزي بتسجيل عملية التبادل ضمن ملف بعد التحقق من التوقيع الرقمي للعميل، وبحيث لا يمكن للعميل إنكار قيامه بعملية التحويل. وبحيث لا يمكن لأي خدمة من خارج النظام انتحال دور أحد العملاء أو إعادة إرسال رسائله.

- بهدف السماح لدخول عدد أكبر من الأعضاء مع المحافظة على وثوقية النظام، يتم الاستغناء عن المفتاح السري، وتشفير نتائج طلبات الاستعلام عبر المفتاح العام لكل عميل، شريطة أن يكون قد أثبت عضويته ضمن النظام حيث تحقق الخدمة المركزية من عضويته صاحب أي طلب من خلال مجموعة من الخدمات الموثوقة المخولة بمنح العضوية.

المطلوب:

تنفيذ هذا النظام باستخدام أي لغة برمجية على شكل خدمات تتواصل عبر الشبكة باستخدام أي بروتوكول مناسب، وبحيث يتم التركيز على تحقيق المتطلبات الأمنية بالدرجة الأولى (لا داعي للاهتمام بسهولة الاستخدام)، وفق المراحل التالية:

1. المرحلة الأولى، تنفيذ عملية الاستعلام مع الحفاظ على خصوصية العملاء (تشفير متناظر مع اقتراح AES)
2. المرحلة الثانية، تنفيذ عملية التحويل مع الحفاظ التأكد من هوية صاحب التحويل وعدم إمكانية نكران عملية التحويل (تشفير غير متناظر مع اقتراح RSA)
3. المرحلة الثالثة : تنفيذ عملية التحويل ولكن باستخدام التشفير الهجين PGP
4. المرحلة الرابعة: تنفيذ عملية التحقق من صحة عضوية أي IP أو اسم نطاق (تطبيق مفهوم الشهادة الالكترونية)

ملاحظات :

1. عدد الطلاب بالغروب 4 كحد أقصى
2. من الطبيعي اعتماد النموذج Client / Server أثناء تصميم النظام
3. كل طالب مسؤول عن الخوارزميات المنفذة وبشكل دقيق
4. تسليم الوظيفة على مراحل وتحدد مواعيد التسليم لاحقاً
5. **كل قسم يلتزم بمواعيد يحددها المدّرس الخاص به**

منسّق العملي	مدرّس العملي
م. زين صالح	م. الأمجد توفيق اصطيف