ملخص :

علم التشفير هو واحد من أكثر العلوم التي لا غنى عنها في ضمان سرية المعلومات المتبادلة. هذا العلم يختص بانشاء ودراسة الخوارزميات التي تؤمن نقل المعلومات عبر الإنترنت. ظهرت خوارزمية جديدة في عام 2011، على غرار خوارزمية 128-bit AES الأصلية, توفر المزيد من الأمن من خلال تعزيز الموثوقية ضد هجوم البحث الشامل في مفتاح التشفير. لكنها لا تستطيع التعامل مع حمل معالجة التشفير الثقيل مع وجود النظم الحديثة ذات الموارد المحدودة. يعرض عملنا تصميم محسن لخوارزمية 512-bit AES يوفر مستوى أمان عالي ويرفع من الأداء عن طريق التقليل من استخدام مساحة الذاكرة المستعملة و الوقت المستغرق في التشفير من أجل القدرة على العمل في خصائص محددة للأنظمة ذات الموارد المحدودة.

الكلمات المفتاحية: علم التشفير، سرية المعلومات المتبادلة، الأنظمة ذات الموارد المحدودة.

Abstract:

The Cryptology is the most indispensable science used in the guarantee of the confidentiality of the exchanged information. It consist of creating and studying algorithms that secure the transmission over the internet. A new algorithm appeared in 2011, similar to the original AES algorithm, provides more security by enhancing the reliability against the brute force attack. However, it cannot handle the heavy encryption-processing load with the existence of the modern resource-limited systems. Our work presents an improvement design of 512-bit AES algorithm that provides high security level and ameliorates the performance by minimizing the use of memory space and time encryption to be able to work in specific characteristics of resource-limited systems.

Keywords: Cryptography, Confidentiality, resource-limited systems.

Résumé :

La cryptologie est la science la plus indispensable utilisé dans la garantie de la confidentialité des informations échangées. Il consiste à créer et étudier des algorithmes qui sécurisent la transmission sur Internet. Un nouvel algorithme est apparu en 2011, similaire à l'algorithme AES original, fournit plus de sécurité en améliorant la fiabilité contre l'attaque de la recherche exhaustive. Cependant, il ne peut pas gérer la lourde charge du processus de chiffrement avec l'existence des systèmes de ressources limitées modernes. Notre travail présente une amélioration de l’algorithme 512-bits AES qui fournit haut niveau de sécurité et améliore les performances en réduisant l'utilisation de l'espace mémoire et le temps de chiffrement pour être en mesure de travailler dans les caractéristiques spécifiques des systèmes de ressources limitées.

Mots clé : Cryptographie, Confidentialité, Systèmes de ressources limités.