Résumé :

Ce mémoire de master Algèbre et Mathématiques discrètes s'inscrit dans le cadre de la théorie des anneaux de polynômes à plusieurs variables et leurs applications en cryptographie asymétrique. On donne tout d'abord des notions générales sur les anneaux et les corps. Par suite, on fait une étude sur l'anneau de polynômes à plusieurs variables. D'autre part, nous avons étudié La cryptographie asymétrique.

Enfin, on s'intéresse au protocole cryptographique asymétrique sur l'anneau de polynômes à plusieurs variables.

Mots clés: Anneau, corps, idéal, l'anneau de polynômes à plusieurs variables, la cryptographie asymétrique.

Abstract :

This master thesis Algebra and Discrete Mathematics is part of the theory of multi-variable polynomial rings and their applications in asymmetric cryptography.

First, general notions about rings and bodies are given. As a result, we study the ring of polynomials with different variables. On the other hand, we studied asymmetric cryptography.

Finally, we are interested in the asymmetric cryptographic protocol on the ring of multivariate polynomials.

Keywords: Ring, filed, ideal, ring of polynomials to more variables, asymmetric cryptography.

ملخص :

هذه مذكرة ماستر الجبر والرياضيات المتقطعة، هي جزء من نظرية الحلقات متعددة الحدود متعددة المتغيرات وتطبيقاتها في تشفير غير متماثل.

أولاً ، يتم إعطاء مفاهيم عامة حول الحلقات والحقول. نتيجة لذلك ، ندرس حلقة كثير الحدود مع متغيرات مختلفة. ومن ناحية أخرى ، درسنا التشفير غير المتماثل.

أخيرًا ، نحن مهتمون ببروتوكول التشفير غير المتماثل على حلقة كثيرات الحدود متعددة المتغيرات.

الكلمات المفتاحية: حلقة ، حقل ، مثالية ، حلقة متعددة الحدود لمزيد من المتغيرات ، تشفير غير متماثل.