أنموذج (أ) الخاص برسائل الماجستير و اطاريح الدكتوراة (اخر شهادة)

University of Baghdad				
College Name	College of dentistry			
Department	Basic sinces			
Full Name as written in Passport	Raghad khalid Mohammed			
e-mail	Raghad_meme@yahoo.com			
Career	◌ Assistant Lecturer	● Lecturer	◌ Assistant Professor	◌ Professor
	● Master	◌ PhD		
Thesis Title	Genetic Algorithms: A Cryptanalysis tool			
Year	2005			
Abstract	Cryptanalysis is the science and study of method of breaking ciphers. A cipher is breakable if its possible to determiner the plaintext or key from the ciphertext, or to determine the key from plaintext-ciphertext pairs. All type of cryptanalysis methods can be considered as searching for smoothing (key, Plaintext,…) Since genetic algorithms are a powerful search method, it means that GAs can be used in the field of cryptanalysis This research is an attempt to study the robustness and weakness using genetic algorithm as cryptanalytic tool. The result show that GA was successful in analyzing the simple substitution cipher, transposition cipher and RSA by finding the exact key i9n all the attempted cases by consuming a small fraction of the search space. All proposed algorithms went through the process of fine tuning the parameters of each GA and testing the work ability of each one. The result indicated that unless all the components of the GA be designed and fitted according to the problem, the GA may not work successfully, saw that for the knapsack problem when the fitness function was not express able. But the results, indicated also that the use of heuristic techniques in the GA as well any knowledge about the problem will improve the efficiency of the GA. Finally the proposed algorithms are programmed by (Delphi Language) to			

	show the results and effects of solving the cryptanalysis tools using genetic algorithms.