UNIVERSITI PUTRA MALAYSIA

CRYPTANALYSIS OF EL-GAMAL AAβ CRYPTOSYSTEM

ARIF BIN MANDANGAN

IPM 2011 17

CRYPTANALYSIS OF EL-GAMAL AA_β CRYPTOSYSTEM

By

ARIF BIN MANDANGAN

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

April 2011

Abstract of thesis presented to the Senate of Universiti Putra Malaysia
in fulfilment of the requirement for the degree of Master of Science

CRYPTANALYSIS OF EL-GAMAL AA_β CRYPTOSYSTEM

By

ARIF BIN MANDANGAN

April 2011

Chair: Muhammad Rezal Kamel Ariffin, PhD

Institute: Institute for Mathematical Research

In this research, we strengthen the security of the El-Gamal AA_β Cryptosystem, simply referred as the AA_β-cryptosystem. The key exchange protocol of the AA_β-cryptosystem is analogous to the Diffie-Hellman key exchange protocol. The encryption and decryption processes of the AA_β-cryptosystem are efficient since the operations involved are the simple addition and subtraction modulo 1.

Unfortunately, the AA_β-cryptosystem was successfully attacked by the passive adversary attack. This attack is manipulating the weaknesses of the public key and encrypting/decrypting keys structure. The hard mathematical problem of the AA_β-cryptosystem has been reduced to the Discrete Logarithm Problem Modulo 1 which can be solved by using the passive adversary attack.

As a solution, we redefined the structure of the public key and encrypting/decrypting keys. We propose a new secret parameter that plays an important role in the computation of the encrypting/decrypting keys. Without the correct combination of the secret parameters, the adversary will not be able to compute the encrypting/decrypting keys.

The Discrete Logarithm Problem Modulo 1 for the strengthened AA_β–cryptosystem is more difficult than the previous one. Now the adversary needs to find two secret parameters and this task could not be done via the passive adversary attack.

Furthermore we propose some attacks which aim to get the secret parameters which are used in the calculation of the encrypting/decrypting keys. Those attacks are the exhaustive search attack on the secret parameters and the linear Diophantine equation attack. We show that these attacks fail to get the correct secret parameters efficiently.

Finally we redefined the hard mathematical problem of the strengthened AA_β-cryptosystem. To break the security of the strengthened AA_β-cryptosystem, one needs to find the private key. By choosing sufficiently large private key size, it is computationally infeasible to reveal the value of the private key via the exhaustive search attack. Therefore, the AA_β-cryptosystem has a potential to be a secure cryptosystem.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Master Sains

ANALISISKRIPTO BAGI SISTEMKRIPTO EL-GAMAL AA_{β}

Oleh

ARIF BIN MANDANGAN

April 2011

Pengerusi: Muhammad Rezal Kamel Ariffin, PhD

Institut: Institut Penyelidikan Matematik

Dalam kajian ini, kami memperkuatkan keselamatan Sistemkripto El-Gamal AA_{β}, secara ringkasnya dirujuk sebagai sistemkripto-AA_{β}. Tatacara pertukaran kekunci bagi sistemkripto-AA_{β} adalah analog kepada tatacara pertukaran kekunci Diffie-Hellman. Proses-proses enkripsi dan dekripsi adalah cekap memandangkan operasi-operasi yang terlibat adalah penambahan dan penolakan modulo 1 yang ringkas.

Malangnya, sistemkripto-AA_{β} telah berjaya diserang dengan serangan musuh pasif. Serangan ini dibangunkan dengan memanipulasi kelemahan-kelemahan struktur kekunci awam dan kekunci mengenkripsi/mengdekripsi. Masalah bermatematik payah bagi sistemkripto-AA_{β} telah diturunkan kepada Masalah Logaritma Diskrit Modulo 1 yang boleh diselesaikan dengan menggunakan serangan musuh pasif.

Sebagai penyelesaian, kami menakrifkan semula struktur kekunci awam dan kekunci mengenkripsi/mengdekripsi. Kami mengajukan satu parameter sulit baharu yang memainkan peranan penting dalam pengiraan kekunci mengenkripsi/mengdekripsi. Tanpa gabungan parameter sulit yang betul, pihak musuh tidak akan dapat mengira kekunci mengenkripsi/mengdekripsi.

Masalah Logaritma Diskrit Modulo 1 bagi sistemkripto-AA_β yang telah diperkuatkan adalah lebih susah berbanding sebelum ini. Sekarang, pihak musuh perlu mencari dua parameter sulit dan tugas ini tidak dapat dilakukan melalui serangan musuh pasif.

Seterusnya kami turut mengajukan beberapa serangan yang bertujuan untuk mendapatkan parameter-parameter sulit yang digunakan dalam pengiraan kekunci mengenkrip/mengdekrip. Serangan-serangan tersebut adalah serangan carian menyeluruh terhadap parameter-parameter sulit dan serangan persamaan Diofantus linear. Kami menunjukkan bahawa serangan-serangan ini gagal untuk mendapatkan parameter-parameter sulit yang betul secara cekap.

Akhirnya kami menakrifkan semula masalah bermatematik payah bagi sistemkripto-AA_β yang telah diperkuatkan. Untuk memecahkan keselamatan sistemkripto-AA_β yang telah diperkuatkan, seseorang perlu mencari kekunci peribadi. Dengan memilih saiz kekunci peribadi yang cukup besar, mendedahkan kekunci peribadi melalui serangan carian menyeluruh adalah tidak dapat terlaksana secara pengiraan. Maka, sistemkripto-AA_β adalah berpotensi untuk menjadi suatu sistemkripto yang selamat.

ACKNOWLEDGEMENTS

First and foremo st, all praise to the almighty ALLAH S.W.T for His blesses and merciful those enable me to enrich my knowledge.

I am sincerely grateful to my supervisor, Dr. Muhammad Rezal Kamel Ariffin, for his patience and kindness for supervising me and his willingness to share his knowledge. Sincere appreciation to my co-supervisors, Assoc. Prof. Dr. Mohd. Rushdan Md. Said and Assoc. Prof. Dr. Azmi Jaafar for giving advice on my research.

To my lovely wife Mrs. Che Haziqah Che Hussin and my dearest son Muhammad Danish Darwish, a lot of thanks and love for giving me soul, energy and moral boast to complete this journey. To my parents, family, lecturers, Prof. Dr. Mohd. Harun Abdullah and Assoc. Prof. Dr. Jumat Sulaiman, thank you very much for giving continuous moral support. Also to my friends especially Zahari Mahad, Mrs. Aniza Abd. Ghani and Mohd. Azlan Daud, thanks for supporting me along this journey.

I want to thank Universiti Putra Malaysia especially Institute for Mathematical Research for providing good research environment. Last but not least, a lot of appreciation to Universiti Malaysia Sabah and Ministry of Higher Education (MOHE) Malaysia for encouragement and financial support.

Thanks for this amazing journey. May Allah S.W.T blessing all of you. Wassalam.

I certify that an Examination Committee has met on **07 April 2011** to conduct the final examination of Arif bin Mandangan on his thesis entitled "**Cryptanalysis on the El-Gamal AA_β cryptosystem"** in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Examination Committee were as follows:

Siti Hasana Sapar, PhD
Faculty of Science
Universiti Putra Malaysia
(Chairperson)

Zanariah Abdul Majid, PhD
Faculty of Science
Universiti Putra Malaysia
(Internal Examiner)

Eddie Shahril Ismail, PhD
Faculty of Science and Technology
Universiti Kebangsaan Malaysia
(External Examiner)

Hailiza Kamarul Haili, PhD
Associate Professor
School of Mathematical Sciences
Universiti Sains Malaysia
(External Examiner)

SHAMSUDDIN SULAIMAN, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of **Master of Science**. The members of Supervisory Committee were as follows:

Muhammad Rezal Kamel Ariffin, PhD
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Mohamad Rushdan Md. Said, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Member)

Azmi Jaafar, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

HASANAH MOHD GHAZALI, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

ARIF BIN MANDANGAN

Date:

TABLE OF CONTENTS