Malaysian Journal of Mathematical Sciences, Volume 11 (S) August 2017
Special Issue: The 5th International Cryptology and Information Security Conference 2016 (CRYPTOLOGY2016)

Preface

Since the time of Julius Caesar and possibly up until the Greek era, cryptography (a word that is derived from the Greek term "cryptos") has been an integral tool for organizations (and indeed for individuals too) to ensure information that is intended only for authorized recipients remain confidential only to this set of people. Cryptography had far reaching implications for organizations in the event information leakage occurred. Often referred to as the "last bastion of defence" – after all other mechanisms had been overcome by an adversary, encrypted information would still remain useless to the attacker (i.e. that is, under the usual security assumptions). Nevertheless, this simple fact has remained oblivious to the practitioners of information security – omitting cryptographic mechanism for data being transferred and also during storage.

Fast forward to World War 2, – the war between cryptographic and cryptanalytic techniques. While the Germans were efficiently transferring information via the Enigma encryption machine, the Allies in Bletchley Park, England were busy intercepting these ciphered information being transmitted via telegraph by the Germans. Leading mathematicians, linguists, engineers etc. were all working to cryptanalyze these ciphers in the most information way. It is here that the first electrical machine (i.e. the "bomba") was born – and revolutionized computing. Post World War 2 saw the emergence of the "computer". Every organization that had to process data had to acquire a computer so as not to be left behind by their competitor. The banking sector advanced on a global scale due to the invention of the computer. Techniques to secure information among the headquarters of these banks had to be developed. Encryption procedures using the same key (i.e. symmetric encryption) played this role in the early days. Then came the unthinkable problem – computers were being deployed almost everywhere. How is it possible to deploy cryptographic keys in secure manner so that symmetric encryption could take place? Thus, leading to the so-called "key distribution" problem. It was not until 1975, when Diffie and Hellman provided us with a secure key exchange method – and in 1976 when Rivest, Shamir and Adleman with the "asymmetric encryption" scheme (i.e. to encrypt using key e and decrypt uing key d, where $e \neq d$). Since then, cryptographic procedures evolved, not only playing the role of ensuring confidentiality of data, but also to ensure integrity and authenticity of data. It is also able to ensure that non-repudiating of data does not occur.

Mechanisms to transfer and store data has changed of the centuries and more so every 5 years (in this modern age). Cryptography that has long existed before mechanisms changed from manual – telegraphic – electrical – electronic (WAN/LAN/internet) – wired until wireless procedures, has to be properly deployed in order to maintain a high level of security confidence among the stakeholders of a certain organization. The concept of securing information via encryption procedures has to be properly understood in order to avoid a null intersection to occur between cryptography and computer security practitioners. This scenario would not be to the best interest for stakeholders. As a "friendly" reminder, this scenario could already been seen in other discipline of knowledge where the "minuting" ("minute-ting") of knowledge has forced the original body of knowledge to look as though it is independent and disassociated. Ever since mass usage of computers became a reality, computer security issues have never been this complicated. However, as the human race advances so will ingenious ideas emerge to overcome challenges.

It is hoped that Cryptology2016 will not only provide a platform for every participant to exchange ideas in their respective fields, but also to exchange new ideas on a broader scale for the advancement of the field of cryptology and computer security. The organizing committee hopes every participant will have an enjoyable and beneficial conference.

The editors would like to thank all participants for their contributed papers. A special thanks to the members of scientific committee and panel of reviewers who had taken the time to review the papers thoroughly and suggesting improvements so as to enhance the quality of papers. Finally, we extend our appreciation for the efforts of conference organiser and everyone whose contributions have made the publication of this special issue in Malaysian Journal of Mathematical Sciences possible.

Thank you.

Guest Editors:
Muhammad Rezal Kamel Ariffin,
Mohamad Rushdan Md. Said,
Hailiza Kamarulhaili,
Goi Bok Min

Formating & Typesetting:
Nor Azlida Aminudin & Amir Hamzah Abd Ghafar