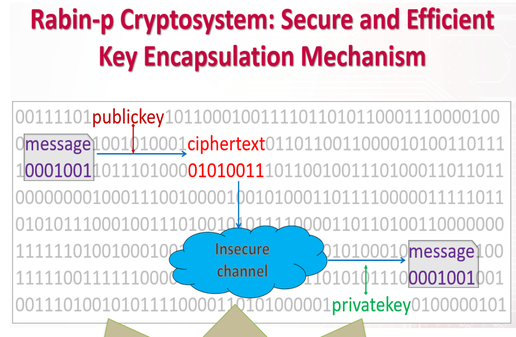
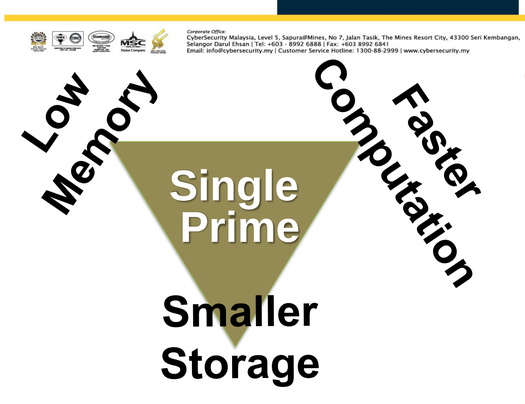
RABIN-p KEY ENCAPSULATION MECHANISM (KEM)

IPR NO: LY2018004527, LY2018004529, +3 More IPR (Filed to MYIPO)



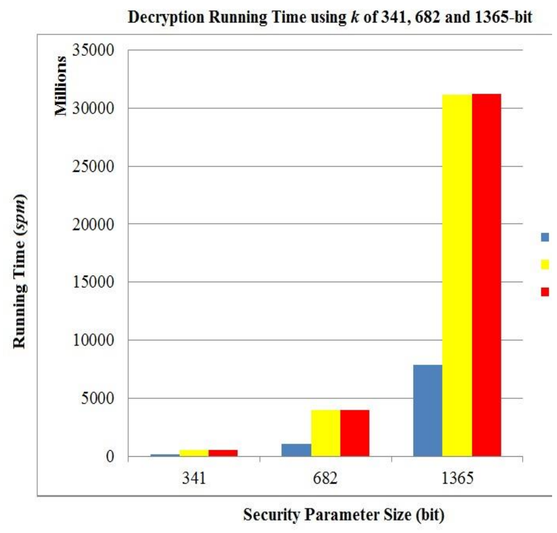
Track records:

- ❑ Undergoes rigorous analysis by Malaysian crypto-experts
- ❑ Short-listed for the National Trusted Cryptographic Algorithm List
- ❑ Approved by CyberSecurity Malaysia



Work Comparison/Competitor(s)

Works	Rabin-p	HIME(R)	RSA-OAEP
Padding mechanism	No	Yes	Yes
Use CRT library	No	Yes	Yes
#decryption exponentiaon	1	2	2
#private key	1	2	4



TECHNOLOGY

A data breach/leaked is the (un)intentional release of secure or private/confidential information to an untrusted environment happens daily. In Malaysia scenario, the main reason for a data breach/leaked is because the data (read: critical infrastructures data) itself is not encrypted in the first place. Thus, a home-grown, fully developed and ready to be deployed public key encryption algorithm is expected to cater to the said problem.

Secure-Efficient-Practical

Rabin-p Key Encapsulation Mechanism (KEM) is design aiming for secure, efficient and practical public key encryption with the following properties:

- the ability to carried large encrypted data
- decryption failure-free guaranteed
- achieves the higher security measure
- easily deployed on software and hardware

ADVANTAGES

- Compared to existing standardized products/technology; Rabin-p KEM use only **single prime number** for decryption, contribute to:
  - low memory consumption (energy-saver)
  - faster running time (low complexity)
  - required less storage and space (cost effective)
- Rabin-p KEM is written in the C/C++/Java/PHP environment to perform the most efficient programming strategies – to meet industry guidelines.

MARKET POTENTIAL

Commercializability

The invention is fully functional, ready for commercialization. Currently collaborate with **IExploTech** as strategic industry partner.

Achievements

- **5** Copyrights, **2** R&D Competition Awards
- **4** Citation Index Publications, **2** Excellent Paper Awards
- Short-listed for the National Trusted Cryptographic Algorithm List under MySEAL initiative spearheaded by CyberSecurity Malaysia (CSM)

Project Leader : Dr. Muhammad Asyraf Asbullah
Team members : Assoc. Prof. Dr. Muhammad Rezal Kamel Ariffin, Zahari Mahad
Institute : Institute for Mathematical Research (INSPEM)
Email : ma_asyraf@upm.edu.my
Phone : 03-9769.6998
Expertise : Mathematical Cryptography, Cryptanalysis