**MOBILE PAYMENTMETHODBASED ON PUBLIC-KEY**

**CRYPTOGRAPHY**

Adnan A. Hnaif and Mohammad A. Alia

Faculty of Science and Information Technology – Al-Zaytoonah University of

Jordan

# *ABSTRACT*

*Mobile payment is defined as mobile money, which is considered as an attractive alternative for cash, cheque, or credit. In this paper we propose a new secure mobile paymentmethod. This method is summarized in three processes: firstly, the authentication process, which involves the authentication phases for the applied customers. Secondly, the member recognition process which tests and ensures the customer membership by the market server. Finally, payment processwhich will be done by ciphering the customer information using public-key encryption cryptosystem (RSA), to be submitted over an insecure network to the market server. Actually, this mobile payment methodis more efficient than otherpayment methods since the customer can pay from his/her own mobilephone without any extra cost and effort. The RSA public-key encryption system ensures the security of the proposed method. However, to prevent a brute force attack, the choice of the key size becomes crucial.*