E-VOTING PROTOCOL BASED ON PUBLIC-KEY

CRYPTOGRAPHY

Hayam K. Al-Anie, Mohammad A. Alia and Adnan A. Hnaif

Faculty of Science and Information Technology – Al Zaytoonah University of Jordan, P.O.Box: 130 Amman (11733) Jordan

drhayam, dr.m.alia, dr.adnan\_hnaif @alzaytoonah.edu.jo

# *ABSTRACT*

*In this paper we propose a new secure E-Voting protocol based on public-key encryption cryptosystem. This protocol is summarized in three processes: firstly, access control process which involves the identification and authentication phases for the applied citizens. Secondly, the voting process which will be done by ciphering the voter information using public-key encryption cryptosystem (RSA), to be submitted over an insecure network to the specified government election server. Finally, the election server administrator will sort the final result by deciphering the received encrypted information using RSA private key. Actually, this E-Voting protocol is more efficient than others E-Voting protocols since the voter can vote from his/her own personal computer (PC) without any extra cost and effort. The RSA public-key encryption system ensures the security of the proposed protocol. However, to prevent a brute force attack, the choice of the key size becomes crucial.*