International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 2, Apr 2014, 133-142

IDENTITY-BASED CRYPTOGRAPHY FOR SECURE MOBILE COMMUNICATION

RUSHIKESH MADHUKAR BAGE & GAURAV DIGAMBAR DOIPHODE

Graduate Student, Department of Computer Science, Mumbai, Maharashtra, India

ABSTRACT

In this paper, an identity-based key agreement system and its implementation for mobile telephony in GSM and UMTS networks is presented. The use of telephone numbers as public keys allows the system to piggyback much of the security overhead for key management to the existing GSM or UMTS infrastructure. The proposed approach offers solutions to the problems of multi-domain key generation, key distribution, multi-domain public parameter distribution and inter-domain key agreement. The feasibility of the approach is illustrated by presenting experimental results based on smartphones. While it is possible to implement end-to-end encryption of mobile phone calls based on a Public Key Infrastructure (PKI), the complexity of setting up and using a PKI is prohibitive, especially since many users of mobile phones are not well versed in cryptographic procedures and are quickly overwhelmed when confronted with public and private keys, certificates, signatures and revocation lists.

KEYWORDS: Cryptography, Security, Mobile, Calls, GSM, UMTS, Identiy-Based, Smartphones