ABSTRACT

Nowadays, all kinds of data are digitalized and the security for the data transmitted through the network is an issue due to the intruders` attack. This project presents the standard for transmitting an encrypted multiple data to the recipient. Here encryption of multiple plain text (message) is processed with multiple random keys that are intended for a single recipient. Encryption and decryption is proposed using modified Elgamal Encryption Algorithm. Random keys are selected from cyclic group, G. This provides a solution to situations requiring an extra level of security through multiple monitoring and multiple controls intended with the collection of individual data. The additional random keys are used for the process that improves the complexity of the algorithm. This limits the chance of breaking the algorithm using brute force or systematic attack.

திட்டச்சுருக்கம்

இப்போதெல்லாம், அனைத்து வகையான தரவுகளும் டிஜிட்டல்மயமாக்கப்பட்டன மற்றும் பிணையம் வழியாக அனுப்பப்படும் தரவு பாதுகாப்பாளர்களின் தாக்குதல் காரணமாக ஒரு சிக்கல். இந்த திட்டம் பெறுநருக்கு ஒரு மறைகுறியாக்கப்பட்ட பல தரவுகளை வழங்குவதற்கான தரநிலையை வழங்குகிறது. இங்கே பல எளிய உரை (செய்தி) குறியாக்கம் ஒரு ஒற்றை பெறுநருக்கு நோக்கம் கொண்ட பல சீரற்ற விசைகள் மூலம் செயலாக்கப்படுகிறது. திருத்தப்பட்ட எல்மால் என்கிரிப்சன் அல்காரிதம் பயன்படுத்தி குறியாக்க மற்றும் குறியாக்கம் பரிந்துரைக்கப்படுகிறது. சுழற்சிக்கான குழுவான G. இவற்றிலிருந்து சீரற்ற விசைகள் தேர்ந்தெடுக்கப்பட்டன. இது பல்வேறு கண்காணிப்பு மற்றும் தனிநபர் தரவு சேகரிப்புடன் கூடிய பல கட்டுப்பாடுகளின் மூலம் கூடுதல் பாதுகாப்பு நிலை தேவைப்படும் சூழ்நிலைகளுக்கு ஒரு தீர்வை வழங்குகிறது. கூடுதல் சீரற்ற விசைகள் வழிமுறை சிக்கலான தன்மையை மேம்படுத்தும் செயல்முறைக்கு பயன்படுத்தப்படுகின்றன. இது முரட்டுத்தனமான அல்லது திட்டமிட்ட தாக்குதல் மூலம் வழிமுறைகளை உடைப்பதற்கான வாய்ப்புகளை கட்டுப்படுத்துகிறது.

LIST OF FIGURES

LIST OF ABBREVIATIONS

DES	Data Encryption Standard
DSA	Digital Signature Algorithm
GF	Galois Field
DLP	Discrete Logarithmic Problem
ECG	Elliptic Curve Group
CCG	Conic Curve Group
DFD	Data Flow Diagram
JDK	Java Development Kit
JRE	Java Runtime Environment
JVM	Java Virtual Machine
SDK	Software Development Kit