The need for new cryptosystems grows in today's increasingly commercializing world. However, contemporary cryptography cannot meet such demand. In this paper, two main cryptographic problems—privacy and authentication—and their possible solutions are discussed.

Comment [S1]: Content: A

Organization: A

Writing: A

Grading Criteria

Content: Does your summary contain the most important information presented in the paper? Is the content correct, or does it contain technical errors?

Organization: Do you have good ordering of the sections/subsections? Are the sections linked together well or do they appear abruptly? Does the paper flow? Did you motivated/introduce/define items appropriately before using them?

Writing: Did you use words and grammar correctly. Does the writing have a clear and easy to understand style?

A privacy system disallows unauthorized parties to obtain information exchanged over public channels, thus ensuring message being read by recipient only. An authentication system ensures no messages with illegitimate senders enter public channels; the problem is subdivided into user authentication and message authentication. Here a public channel may be threatened by eavesdropping or injection or both; some channels are more vulnerable to the former threat, such as radio, some to the latter, such as telephone communication.

The conventional cryptosystem used for privacy involves an invertible transformation, converting plaintext to ciphertext using key, which is exchanged over private channel beforehand. A system may be computationally or unconditionally secure. The latter, such as one time pad, results from multi-solution interpreted from ciphertext; such system is definitely secure, but too impractical for many applications. Cryptosystems can also be categorized as stream ciphers, which process the plaintext in small chunks, and block ciphers, which manipulate large blocks of text such that small change in input severely affects output (error-propagation property).

For authentication system, to ensure no meddlers can inject messages, information including date and time are attached to the original message and key. Such authenticity is enforced by the error-propagation of ciphertext.

The first step in judging the security level of a cryptosystem is to examine what type of threats to which it succumb. In ciphertext only attack, the cryptanalyst only knows some statistical language properties; this is the weakest attacks. In known plaintext attack, the cryptanalyst passively obtains the plaintext and interpret to get the key; systems succumbing to such threat have to keep their past messages secret, which is unrealistic in commercial and diplomatic situations. In chosen plaintext attack, often called an IFF attack, enemy cryptanalysts send challenges and find the authentication key in use by examining the encrypted responses. Besides, threat of compromise of the receiver's authentication data lays in the security vulnerability of receiver's password tables; threat of dispute is arisen from people denying sent messages, or claiming nonexistent sent messages.

Nowadays, conventional cryptosystem is no longer useful, as key-exchanging via private channels are unrealistic for users with no prior acquaintance. Two techniques are invented to address this problem.

First is the public key cryptosystem; this involves two inverse algorithms E_k and D_k , both easily computed from k, and used for easily encrypting/decrypting messages; but it is hard to derive D_k from E_k. User's E_k is released to public and everyone can encrypt messages and send to him, but only he has a private key to decrypt received messages; it is feasible to generate E_k-D_k pairs from k as well. For example, the matrix inversion approach, though not much of practical use, clarifies the ratio of "cryptanalytic" time to enciphering/deciphering time must be large. Another example makes use of the difficulty of analyzing programs in low level languages.

Second is the public key distribution system; it makes two users successfully exchange a key over insecure channels. Merkle's solution to this problem has high transmission overhead and may be practical only under high bandwidth data links. But a new solution requires only one key to be exchanged: users i and j have their respective private keys X_i and X_j and public keys Y_i and Y_j; a common key K_{ij} is derived by Y_j^{Xi}modq and Y_i^{Xj}modq respectively; but it is computationally infeasible to obtain K_{ij} only from Y_i and Y_j by a third party.

Today's business transactions require the use of digital signatures; it is easy for everyone to recognize but impossible for non-legitimate signer to produce it; such technique is called one-way authentication. For instance, a traditional way of dealing with "login" problem is to keep the password directory but this is highly insecure. So new authentication procedures of getting passwords without knowing them appear; password input into function f to obtain f(PW), afterwards any user-entered passwords at login are computed by f to see if results are identical with f(PW); f is a one-way function as computing f^{-1} is infeasible; polynomials might be good choice for f. Another way of one-way authentication is as follows: user A uses his private key to encrypt a message; others can recover A's original message using A's public key; this further prevents the threat of dispute. In fact, for one-way message authentication, a technique using one-way function mapping k-dimensional binary space into itself for k on the degree of 100 can be employed as partial solution; for one-way user authentication, user gives system f^T(PW) and at time t the appropriate authenticator is f^{T-t}(PW), whilst the system calculates by f^t(PW).

From proven results, we could see that one-way function can be produced by cryptosystem against known plaintext attack and a public key cryptosystem can be used to generate a one-way authentication system, but their converses are not necessarily true. It is also noted that some cryptosystems, named "trap doors", can be broken by their designers who hold the "trap-door information", which is the knowledge of key-computing algorithm; and this is undesirable. Later a concept "quasi" arises to refer to function or cipher that is computationally unachievable even for the designers to find the decrypting key.

Cryptography evolves through many centuries. It is until recent century when people realize none of the cryptosystems developed are unconditionally secure; then the sub-fields which study the complexity of algorithms develops; problems are divided into P and NP classes depending on their solvability in polynomial time by current computers. General cryptanalytic problems are then observed to be NP complete; but this may be insufficient to show that they are cryptographically useful as only worst case analysis is performed on them.

Historical development shows that good cryptography should ensure secrecy and cause no inconvenience on use. The invention of computer boosts its development. Also, there is no clear-cut division between amateurs and professionals in this field.