4C. explain what would happen if the sender and receiver did not agree the details of the protocol.

If a packet from the sender does not reach the receiver, **the sender continues to send subsequent packets until it has emptied its window**. The receiver continues to fill its receiving window with the subsequent packets, replying each time with an ACK containing the sequence number of the earliest missing packet.

➢ Communication protocols with untraceability of sender and receiver

- Previous research on information security has focused on the protection of the contents of messages. But in many cases it is equally important to protect the identities of the sender and receiver and also the time of message transmission.

- This paper proposes communication protocols which make it impossible both for the entities other than the right receiver to decipher the message and for any third party to identify the communicating entities. Since it is impossible in these protocols for any third party to identify the communicators, the protocols are classified into four groups according to whether or not the communicating pair can identify each other. In addition, the security, the implementability, and the mutual relationship of these four kinds of communication protocols are studied.

➢ Negative Acknowledgement:

- In data networking, telecommunications, and computer buses, an **acknowledgment** (**ACK**) is a signal that is passed between communicating processes, computers, or devices to signify acknowledgment, or receipt of message, as part of a communications protocol. The **negative-acknowledgment** (**NAK** or **NACK**[1]) is a signal that is sent to reject a previously received message or to indicate some kind of error. Acknowledgments and negative acknowledgments inform a sender of the receiver's state so that it can adjust its own state accordingly.
- Many protocols contain checksums to verify the integrity of the payload and header. Checksums are used to detect data corruption. If a message is received with an invalid checksum (that is, the data received would have a different checksum than the message had), the receiver can know that some information was corrupted. Most often, when checksums are employed, a corrupted message received will either not be served an ACK signal, or will be served a NAK signal.

➢ Acknowledgment characters:

ASCII code includes an ACK character (0000110_2 or 6_{16}) which can be transmitted to indicate successful receipt and a NAK character (0010101_2 or 15_{16}) which can be transmitted to indicate an inability or failure to receive.[2] Unicode provides visible symbols for these characters, U+2406 (␆) and U+2415 (␕).

➢ Protocol usage:

- Many protocols are acknowledgment-based, meaning that they positively acknowledge receipt of messages. The internet's Transmission Control Protocol (TCP) is an example of an acknowledgment-based protocol. When computers communicate via TCP, received packets are acknowledged by sending back a packet with an ACK bit set. The TCP protocol allows these acknowledgments to be included with data that is sent in the opposite direction.
- Some protocols send a single acknowledgment per packet of information. Other protocols such as TCP and ZMODEM allow many packets to be transmitted before receiving acknowledgment for any of them, a procedure necessary to fill high bandwidth-delay product links with a large number of bytes in flight.