

KRIPTOGRAFI DALAM KESELAMATAN DATA

Arahan: Isikan jawapan pada ruang yang disediakan

Bahagian A

Perkhidmatan Keselamatan	Kepentingan
1. Kerahsiaan	Kesulitan sesuatu maklumat yang dihantar melalui rangkaian [redacted] yang perlu dilindungi supaya maklumat tersebut tidak diketahui oleh pihak lain selain [redacted].
2. Pengesahan	Pengenalpastian pihak-pihak yang terlibat dalam sesuatu [redacted]
3. Integriti	Perkhidmatan [redacted] yang mengenalpasti sebarang perubahan terhadap [redacted] atau [redacted] oleh pihak lain.
4. Tiada Sangkalan	Membuktikan [redacted] dan [redacted] tidak menafikan bahawa mereka menghantar dan menerima maklumat tersebut.

Bahagian B

1. Sifer [redacted]

- Digunakan dalam sifer moden
- Melibatkan kunci awam dan kunci persendirian

2. Sifer [redacted]

- Digunakan dalam sifer klasik
- Menggunakan kunci yang sama untuk melakukan penyulitan dan nyahsulit