Latihan UAS

1. Bukalah situs enkripsi DES online berikut: http://des.online-domain-tools.com/
   Enkripsi pesan dua baris berikut:

   ```
   Ada sindikat narkoba di Bandung
   Tolong selidiki
   ```

   dengan DES. Mode yang digunakan CBC,
   init vector (IV) = `82 9b 36 ba bd 21 be 51`,
   kunci = `rahasia`.

   Tuliskan cipherteksnya dalam kode Hexadecimal

2. Bukalah situs enkripsi AES online berikut: https://encode-decode.com/aes-128-ecb-encrypt-online/
   Dekripsi cipherteks berikut:

   ```
   W8HHQrEQ227h+S85JFKsAvbg/e/eutDRtNZPZIYRlbsTMQrvjXtzp/AWXEZyvZvq
   ```

   dengan AE-128 mode ECB, kunci = detakdetik. Tuliskan plainteks yang dihasilkan.

3. Diketahui pasangan kunci public dan kunci privat kepunyaan Alice dan Bob sebagai berikut:

   Alice:
   Kunci public: (e, n) = (25,667)
   Kunci privat: (d, n) = (961,667)

   Bob:
   Kunci public: (e, n) = (41,391)
   Kunci privat: (d, n) = (601,391)

   Bob mengirim pesan berikut kepada Alice: `BALI`
   (a) Kodekan pesan menjadi integer dengan memisalkan A = 00, B = 01, C = 02, ..., Z = 25
   (b) Tuliskan cipherteks yang dikirim oleh Bob kepada Alice dalam bentuk integer (gunakan calculator di computer)
   (c) Tuliskan hasil perhitungan plainteks yang diterima oleh Alice

4. Diketahui kunci publik RSA milik Bob adalah adalah (e, n) = (5, 221). Alice menegnkripsi pesan dengan kunci public Bob tersebut. Misalkan Carol menyadap komunikasi Alice dan Bob dan berhasil memperoleh cipherteks dari Alice yaitu c = 153. Tentukan plainteks yang berhasil didekripsi oleh Carol dari cipherteks tersebut

5. Misalkan kunci public dan kunci privat Bob dengan algoritma RSA sudah dibangkitkan sebagai berikut (format PEM):

   -----BEGIN PUBLIC KEY-----
   MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJzTg1Y8lZzG5iFEcKkcfU6aLs7CNP31
   /ksr5jQMb0/WEnETEgocTu0pMufT57Cem4WoO6MKpLbZwEEw0+tUB6cCAwEAAQ==
   -----END PUBLIC KEY-----

   -----BEGIN RSA PRIVATE KEY-----
   MIIBVQIBADANBgkqhkiG9w0BAQEFAASCAT8wggE7AgEAAkEAnNODVjyVnMbmIURw
   qRx9TpouzsI0/fX+SyvmNAxvT9YScRMSChxO7Sky59PnsJ6bhag7owqkttnAQTDT
   61QHpwIDAQABAkEAi/S7Vh+1SXe78t54SIOzVI2GzmBFGIwLSBzCUZrzT+QLXpN1
   ga+R2HwvJ2EFofViVB6lQ5hsjgZGpyfHKqFKeQIhAOjWFoI3GuK9R/odChEke6tq
   fyEu8Wx3nDP7hREY0apVAiEArG2Wsc+zV7YDmcfQzmf8hhQt5h29qP0oFrYxq7os
   3gsCIAz09PW0GVPq0pmRiiDgFd25JG/1S8wMb+3YnlQQPIKtAiB83rxENvtVKM5A
   vtD7uZjJ7LE0thMU34j5saYVDDXT8wIhANIxddgPfF52KyhwK8iKn1ealEQnHGw/
   8lsSUTlsFXmi
   -----END RSA PRIVATE KEY-----

   Pesan yang dienkripsi adalah sbb (copas saja):
   ```
   Kita bikin romantis
   Biar makin romantis
   ```

   Tuliskan cipherteks hasil enkripsinya:
   (a) dalam format base64
   (b) dalam format hex

6. Bukalah situs https://codebeautify.org/md5-hash-generator untuk menghitung nilai hash (message digest). Lalu hitung nilai hash untuk pesan berikut:

   ```
   Semoga Indonesia menjadi negara yang adil dan makmur,
   damai sentosa, serta diberkahi oleh Tuhan yang  Mahas
   Esa
   ```

   (a) Dengan MD5
   (b) Dengan SHA-1
   (c) Dengan SHA-256
   (d) Ubah pesan dengan mengubah `Semoga` menjadi `Semogi`, lalu tentukan nilai hash-nya dengan SHA-1

7. Dengan menggunakan situs yang sama seperti pada soal nomor 5, tentukan nilai hash dari file materi kuliah 10-AES-2024.pdf (unduh dari web

https://informatika.stei.itb.ac.id/~rinaldi.munir/Tambahan/tambahan.htm) materi nomor 10, dengan menggunakan SHA-256.

8. Bukalah situs https://www.freeformatter.com/hmac-generator.html untuk menghitung nilai MAC pesan. Hitung nilai MAC untuk pesan AYO KITA PULANG KAMPUNG
   Kunci yang digunakan AKUTAKUTPADAMU
   Fungsi hash yang digunakan SHA-512

9. Bukalah situs Traveloka.com dengan browser chrome, lalu carilah sertifikat digital server situs tersebut.
   (a) Tuliskan nama CA yang memberikan sertifikat digital server Traveloka.com
   (b) Tuliskan masa berlaku sertifikat digital tersebut
   (c) Tuliskan kunci public server traveloka.com
   (d) Tuliskan algoritma yang digunakan untuk tanda-tangan digital
   (e) Tuliskan tanda-tangan digital di dalam sertifikat tersebut
   (f) Tuliskan kunci public CA

10. Alice mengirim pesan APA KABAR BOB kepada Bob. Bangkitkan tanda-tangan digital untuk pesan tersebut dengan menggunakan calculator online.