IDATT2503 - Cryptography Assigment 5

Edvard Berdal Eek

November 2025

Task 1

Alice and Bob want to have an common key using Diffie-Hellmann key exchange. They agree on using the prime $p = 101$, and base $n = 3$. Alice choosed her secret $a = 33$, and Bob chooses $b = 65$.

a) Write a program that prints out all the powers 3^i for $i = 1, ..., 100$. Do the same for 5^i. What is a major difference between these two sequences?

```
-- Base-3 powers in range i = 1, ..., 20 --
3^1: 3
3^2: 9
3^3: 27
3^4: 81
3^5: 243
3^6: 729
3^7: 2187
3^8: 6561
3^9: 19683
3^10: 59049
3^11: 177147
3^12: 531441
3^13: 1594323
3^14: 4782969
3^15: 14348907
3^16: 43046721
3^17: 129140163
3^18: 387420489
3^19: 1162261467
3^20: 3486784401
```

(a) Base-3 powers in range 1-20

```
-- Base-5 powers in range i = 1, ..., 20 --
5^1: 5
5^2: 25
5^3: 125
5^4: 625
5^5: 3125
5^6: 15625
5^7: 78125
5^8: 390625
5^9: 1953125
5^10: 9765625
5^11: 48828125
5^12: 244140625
5^13: 1220703125
5^14: 6103515625
5^15: 30517578125
5^16: 152587890625
5^17: 762939453125
5^18: 3814697265625
5^19: 19073486328125
5^20: 95367431640625
```

(b) Base-5 powers in range 1-20

Looking at the output we can see that the major difference between the sequences is that all the base-5 powers end with a 5.

```
-- Base-3 powers with p = 101 in range i = 1, ..., 100 --
3 9 27 81 41 22 66 97 89 65 94 80 38 13 39 16 48 43 28 84 50 49 46 37 10 30 90 68 2 6 18 54 61 82 44
31 93 77 29 87 59 76 26 78 32 96 86 56 67 100 98 92 74 20 60 79 35 4 12 36 7 21 63 88 62 85 53 58 73
17 51 52 55 64 91 71 11 33 99 95 83 47 40 19 57 70 8 24 72 14 42 25 75 23 69 5 15 45 34 1
Number of distinct residues: 100

-- Base-5 powers with p = 101 in range i = 1, ..., 100 --
5 25 24 19 95 71 52 58 88 36 79 92 56 78 87 31 54 68 37 84 16 80 97 81 1 5 25 24 19 95 71 52 58 88 36
 79 92 56 78 87 31 54 68 37 84 16 80 97 81 1 5 25 24 19 95 71 52 58 88 36 79 92 56 78 87 31 54 68 37
84 16 80 97 81 1 5 25 24 19 95 71 52 58 88 36 79 92 56 78 87 31 54 68 37 84 16 80 97 81 1
Number of distinct residues: 25
```

Figure 2: Base-3 and 5 power residues

If look at the modular residues with prime $p = 101$ we see that the base-5 sequence only has 25 distinct residues (order of 25). The base-3 sequence on the other hand has the order 100.

b) Find their common key.

$$K \equiv n^{ab} \bmod p$$
$$K \equiv 3^{33 \cdot 65} \bmod 101 \equiv 32$$

Task 2

Alice uses $p = 47$, $q = 83$, and $e = 3$ as the public key for her RSA-based signature.

1. What is the Alice's private key?

   To find Alice's private key i needed to find the multiplicative inverse d of e modulo $(p-1)(q-1)$.

   $$d \cdot e \equiv 1 \bmod (p-1)(q-1) \Rightarrow d = 2515$$

   I found this using Python:

   ```
   def mul_inverse(a, n):
     for i in range(n):
       if(a*i % n == 1):
         return i
   ```

   I then printed the key:

   ```
   1. Private key
   k_priv (p, q, d): (47, 83, 2515)
   ```

   Figure 3: Alice's private key

2. Verify if 964 is a valid signature of Alice for the message 100.

   I made yet another Python function now to verify if a signature is valid for a message.

   ```
   def verify(c, m, n, d):
       return c**d % n == m
   ```

This resulted in the output:

```
2. Verify message
Is signature 964 valid for message 100: True
```

Figure 4: Verify message signature output

So the signature was not valid.

3. Alice wants to encrypt and sign the message 100 to Bob. What are the exact steps? Assume Bob has the RSA with public key $(n_B, e_B) = (3127, 33)$.

   Python function for encryption:

```
def encrypt(m, n, e):
    return m**e % n
```

   This resulted in the output:

```
3. Encrypt message
Encrypted message 100 with public key (3127, 33): 487
```

Figure 5: Encryption output

   The encrypted message is 1344, but Bob is not able to decrypt it with public key $(n_B, e_B) = (3127, 33)$.

Task 3

Give a brief comparison of MACs and digital signatures, with respect to purpose, use cases, type of encryption etc

Message Authentication Codes, MACs, provide security through a single shared symmetric key, whilst digital signatures use asymmetric key pair with shared public keys and private keys.

Task 4

1. **Name the two parts/layers of TLS 1.3, and what their purporses are.**

   TLS 1.3 is a cryptographic protocol designed to provide secure communication over the internet. It is designed on top of TCP and consits of two main protocols: Handshake protocol and Record Protocol.

   The handshake protocol is responsible for establishing a secure connection between client and server. I does this using asymmetric encryption. The goal is to authenticate each other and to establish a session key for later.

   The record protocol is responsible for the secure transmission of application data. It uses the symmetric session key derived from the handshake protocol to encrypt and decrypt all subsequent messages while messsage authentication codes (MACs) prevent tampering.

2. **Explain how TLS uses both symmetric and asymmetric cryptography.**

   The way TLS utilizes asymmetric cryptography during the establishment of the connection (handshake protocol) and symmetric cryptography during the connection (record protocol).