# 1 Multiple Choice Answers

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1c) | 2b) | 3a) | 4d) | 5a) | 6d) | 7a) | 8c) | 9c) | 10b) |
| 11d) | 12d) | 13d) | 14a) | 15c) | 16d) | 17a) | 18b) | 19d) | 20d) |
| 21c) | 22a) | 23b) | 24a) | 25a) | 26d) | 27a) | 28d) | 29a) | 30a) |

# 2 Long Answers

**Exercise 1**

**a)** Assume that the length of the alphabet is 26.

**Hill Cipher** There are $26^9$ possible $3 \times 3$ matrices modulo 26. However, not all of them are invertible, and so not all of them can be keys. By the Chinese Remainder Theorem matrices are invertible modulo 26 if and only if they are invertible modulo 13.

How many invertible matrices modulo $n$ are there? A matrix is invertible modulo $n$ if all its columns are linearly independent, i.e. not multiples of each other modulo $n$. This gives us a way of counting all the invertible matrices modulo $n$: for the first column we can choose any three values $(a, b, c)$, the only value we need to exclude is $(0, 0, 0)$. Thus, we have $n$ possibilities for the first entry of the column, $n$ for the second, and $n$ for the third, and we need to deduct 1 from the total. Thus, for the first column we have $n^3 - 1$ possibilities. For the second column we can choose any column that is not a multiple of the first one. Thus, if $(a, b, c)$ is the first column, then we cannot have any column of the form $i \cdot (a, b, c)$ for $i = 0, \ldots, n-1$ as the second column. There are $n$ columns of this form. Thus, for the second column we have $n^3 - n$ possibilities. Similarly, for the third column we can have any column that is not the sum of multiples of the first and the second column. There are $n^3 - n^2$ many columns that are not linearly dependent on the first two. Thus, in total, there are

$$(n^3 - 1)(n^3 - n)(n^3 - n^2)$$

many invertible matrices modulo $n$. Thus we have

$$(2^3 - 1)(2^3 - 2)(2^3 - 2^2) = (8 - 1)(8 - 2)(8 - 4) = 7 \cdot 6 \cdot 4 = 168$$

$3 \times 3$ matrices that are invertible modulo 2, and

$$(13^3 - 1)(13^3 - 13)(13^3 - 13^2) = 9726417792$$

many invertible matrices modulo 13. The total number of invertible matrices modulo 26 is the product of those two numbers, that is

$$(2^3 - 1)(2^3 - 2)(2^3 - 2^2)(13^3 - 1)(13^3 - 13)(13^3 - 13^2) = 9726417792$$

**Random Substitution Cipher** There are 26! possible keys.

**Simple Transposition Cipher** There are 10! possible keys.

**b) Hill Cipher** A ciphertext-only attack can be run as follows: since the key of the Hill cipher is a $3 \times 3$ matrix, it will preserve some di- and trigrams from the plaintext and the ciphertext. If the ciphertext is long enough, one might notice that some groups of letters appear more often than others. We know that in the English language THE is the most common trigram, AND is the second most common trigram, and THA is the third most common one. So, at first, we would run a statistical analysis on the ciphertext to find the three most common trigrams there. There is a chance that the most common trigram in the ciphertext corresponds to the most common trigram in the plaintext, the second most common trigram in the ciphertext corresponds to the second most common trigram in the plaintext, and so on. Assume that the most common trigram in the ciphertext is $x_1x_2x_3$, and the second most common is $x_3x_4x_5$ and the third is $x_6x_7x_8$. Then we can guess that we have the ciphertext-plaintext pair

$$P = \begin{pmatrix} T & A & T \\ H & N & H \\ E & D & A \end{pmatrix} \text{ and } C = \begin{pmatrix} x_1 & x_4 & x_7 \\ x_2 & x_5 & x_8 \\ x_3 & x_6 & x_4 \end{pmatrix}.$$

We can use this ciphertext-plaintext pair to calculate the secret key via $K = CP^{-1}$.

**Random Simple Substitution Cipher** If we choose the plaintext that has the 26 characters of the alphabet, then we see to which ciphertext character all of the plaintext characters get matched. So a ciphertext with 26 characters would be enough in a chosen-plaintext attack, to obtain the complete key. Indeed, a chosen plaintext with 25 characters would be enough, since we then can directly guess the 26th character.

**Simple Transposition Cipher** For the simple transposition a plaintext with 10 different characters is sufficient to find the permutation. Thus, a chosen plaintext attack will give the key by choosing 10 different characters. A known plaintext attack might leave some ambiguity after 10 characters if some of them are the same, so more plaintext/ciphertext pairs may be needed.

**Exercise 2**

**a)**

$$P_t = O_t \oplus C_t \oplus C_{t-1}.$$

**b)** Since the block $C_t$ is needed in the decryption of the block $P_{t+1}$, and the operation performed is a bit-wise XOR, the same bits that have been flipped in $C_t$ will be flipped in $P_{t-1}$.

**c)** Encryption is not possible in parallel, since the encryption of the next block always requires the result of the encryption of the previous block. Decryption is possible in parallel, since only pre-computed values are needed in this operation.

**Exercise 3**

**a)** We first compute $d \pmod{p-1}$ and $d \pmod{q-1}$. We have

$$\begin{aligned} d &\pmod{p-1} \equiv 11 \pmod 4 \equiv 3 \\ d &\pmod{q-1} \equiv 11 \pmod{10} \equiv 1 \end{aligned}$$

Thus, we obtain

$$\begin{aligned} M_p &\equiv C^{d \pmod{p-1}} \pmod p \equiv 2^3 \pmod 5 \equiv 8 \pmod 5 \equiv 3 \\ M_q &\equiv C^{d \pmod{q-1}} \pmod q \equiv 2^1 \pmod{11} \equiv 2. \end{aligned}$$

**b)** By the CRT the decryption result is given as

$$M = q(q^{-1} \pmod p)M_p + p(p^{-1} \pmod q)M_q.$$

We can calculate $q^{-1} \pmod p$ and $p^{-1} \pmod q$ via the Extended Euclidean Algorithm. We obtain as values $q^{-1} \pmod p \equiv 11^{-1} \pmod 5 \equiv 1$ and $p^{-1} \pmod q \equiv 5^{-1} \pmod{11} \equiv 9$. Thus, we obtain

$$M \equiv 11 \cdot 1 \cdot 3 + 5 \cdot 9 \cdot 2 \equiv 33 + 90 = 123 \equiv 13 \pmod{55}.$$

**c)** Yes, the CRT can be used to speed up decryption. Decryption is the most expensive process, since it requires exponentiation by potentially very large numbers: applying the CRT means that we can split this step in two, and instead of performing an exponentiation with one very large number, we can perform two exponentiations with two smaller numbers.

**Exercise 4**

**a)** A value $g$ is a generator modulo $p$ if for $p-1 = n_1^{e_1} \cdot \ldots \cdot n_k^{e_k}$, we have the following:

$$g^{\frac{p-1}{n_i}} \not\equiv 1 \pmod{n}, \text{ for } i = 1, \ldots, k.$$

We have $16 = 2^4$, that is 16 only has one distinct prime factor. Thus, to know whether any value 2 is a generator, we just need to compute

$$2^{\frac{16}{2}} \equiv 2^8 \equiv 256 \equiv 1 \pmod{17}.$$

So, 2 is not a generator. However, we have

$$3^{\frac{16}{2}} \equiv 3^8 \equiv 6561 \equiv 16 \not\equiv 1 \pmod{17}.$$

Thus, 3 is a generator.

Listing all values is also an acceptable answer.

**b)** In the Diffie-Hellman key exchange, $A$ first computes $g^A \pmod{p}$ and sends it to $B$. In this case, $A$ computes $3^3 \equiv 27 \equiv 10 \pmod{17}$. $B$ receives $g^a \equiv 10 \pmod{17}$ and computes $g^b \equiv y \pmod{17}$. $B$ sends $y$ to Alice. Now $A$ can compute the shared secret $g^{ab} \equiv (g^b)^a \equiv y^a \equiv 4^3 \equiv 64 \equiv 13 \pmod{17}$, and $B$ can compute the shared secret as $(g^a)^b \equiv 10^b \pmod{17}$. Since exponentiation is commutative, that is $(g^a)^b = (g^b)^a = g^{ab}$ they both obtain the same shared secret, which is 13.

**Exercise 5**

**a)** It cannot authenticate itself, and the server cannot verfiy its identitiy. Assume there is a legitimate client $A$ and another client $B$. If $A$ does not use a certificate, then $B$ could use $A$'s public key to authenticate to the server: the server would have no way of verifying that $B$ is indeed who he claims, and therefore would allow the connection.

**b)** An advantage is flexibility and backwards compatibility: due to technological advances, the security level of a ciphertextsuite may decrease with time. Attacks may be found, and if we only allow one ciphersuite, the broken cipher suite would have to be switched out for another one, and all hardware would have to be revoked and reprogrammed. Having multiple ciphersuites allows for easy switches if one becomes broken, but also allows for backward compatibility for clients who can only use weaker ciphersuites.

On the other hand, this makes downgrading attacks possible: a malicious client could try to convince the server that it only can use an insecure

ciphersuite. For backwards compatibility reasons, the server would then initiate the connection via the insecure ciphersuite, which the malicious client would be able to break.

**c)** The advantage is that we can have a faster connection. The disadvantage is that it can enable certain types of replay attacks.