# Practice Session 1

Number Theory

Security and Cryptography (CS4520)

1. **Number Theory** *(0 points)*
   For the following questions show all numerical steps and provide the explanation.
   (a) Calculate $\Phi(30)$ and list the set members.
   (b) Give the set of co-primes to 28. How can you calculate the number of elements of this set without listing?
   (c) Give the set of co-primes to 11. How can you calculate the number of elements of this set without listing?
   (d) Compute $gcd(2001, 1150)$ using Euclidean algorithm.
   (e) Compute $33^{34} \bmod 35$.
   (f) Solve the following system of linear congruences:
   $$\begin{aligned} x &\equiv 1 \mod 15 \\ 3x &\equiv 2 \mod 16 \\ 5x &\equiv 3 \mod 17 \end{aligned}$$
   (g) Find the smallest and the largest generators of the cyclic group $(\mathbb{Z}_{19}^*, \cdot)$.
   (h) Find the 7th root of 23 in modulo 143, i.e., find $x$ such that $x \equiv 23^{1/7} \bmod 143$.
   (i) Compute the Jacobi symbol $\left(\frac{4191}{2017}\right)$.

2. **Elliptic Curves** *(0 points)*
   For $F : y^2 = x^3 + 2x + 1 \bmod 11$:
   (a) Check whether this curve is valid or not.
   (b) Check whether $P = (3, 9)$ is on the curve or not.
   (c) Check whether $P = (3, 1)$ is on the curve or not.
   (d) Calculate the addition of $P_1 = (3, 10)$ and $P_2 = (5, 2)$.
   (e) Calculate $2P_1$.
   (f) Calculate $2P_1 + P_1$ .
   (g) Calculate $P_1 - P_1$. Explain the results.

# Practice Session 2

## Classical Systems and Information Theoretic Security
## Security and Cryptography (CS4520)

1. **Permutation Cipher**

   Break the following ciphertext and recover the plaintext:

   UMANH EINGBA REM SMBEREO FA W SOLEH; NC REITIONA FO NEO SSENEEA NDC OULS; FO NEI EMBEMI SA FRLICTFDW ITEP AINH; THERO EMBEMSU NERSYW IALR EMLINA; FY OUI AVEN HS YMPOTHYF ARH UMONP AIAN; HEN ATEO FH MMANY UUC ANOOTR ENAINT

2. **Caesar Shift Cipher**

   Break the following ciphertext and recover the plaintext:

   BMFY NX FKKQZJSHJ? IJHWJFXNSL DTZW BNXMJX, FSI GJNSL XFYNXKNJI BNYM BMFY NX JSTZLM KTW DTZ.

3. **Vigenere Cipher**

   Use Kasiski analysis to break the code used to encrypt the intercept given below, given that it has been encrypted with a Vigenere encryption.

   Auge y bxwfcxc xl wrpk shbrt eiwemsttrnwr, mg kj awtrtgu ztyseg zr xl wrpk. Rwx qrvyms hj pjrlvbrt vvvi bw pccjtw e pquc dk e pkgftk. Xug tfpgkrf kcmm mf erjaxh pkgftkxrzk. Rwx guceet fexgj rwx qrujyvx lntu rd kinf. Jmbxsag nfd peavj rd kinf zr bnwg eyyczi vv syrd se fvagrtg. Jfu ih guceet bx octi xl e fgtptm. Fbvy rwx trtjmc mlnv jccww gjv ktlwniv ycw xug flt mlnv xcil mg uymjeh xpfu iai fgtptm ana km raeaiv gi, uyg qkftk trqgjt llbwcb chx og rzax xb. Ukssrmai kft vmcjvpixbg vf bxlgbxvp iai fgtptm mf erjaxh ptpnitrnnpqxl.

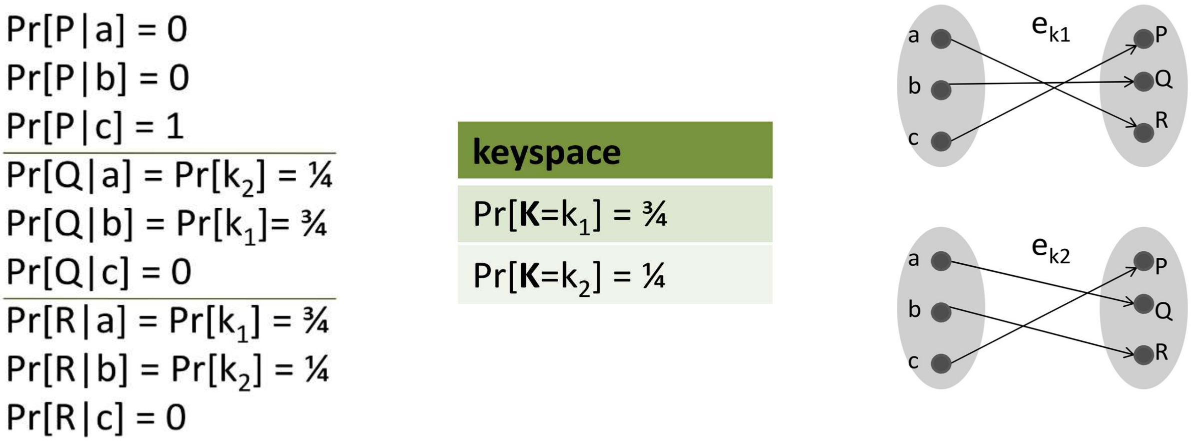
   Hvhwcgxrg vpntl ss eiwemsttrnwr gnp sc ttwvgi mg aeefvp ih yfg rls vea jzbt mlr uvagxx zgjqpzi ogkrtk se yfphx. Gvrycgl yfg r itr auktf xl e fgtptm xuck fxwif vyc hxgegk ktlwnivq. Iai ptpnihkecgfxv qrvyms girf emi ui fgtptm. Zntzmjl trqgjt vea wjc iai fcdc bxxuqu zjm hvhwcgxrg mvwh, ls gjvw rtraqk ptth rctf dmlrt'j ktlwnivq. Hbrpg kft Verurp rbtugi fpl sanp yh feaa bcnl ef vyc cnqogi mu eigvvph br gjv yailndvr, xm mf grqxec ptrazxh oa kpnbrt ccj iai xgpq. Rbtugiq iaeg ccjdp fvncgdgw bh bcnl eeg tppvorf sw bhvr efkeeik ovrwhhf.

4. **Perfect Secrecy**

   Given the plaintext, ciphertext, and key distributions given in Figure 1, compute the posteriori probabilities. Is the encryption perfectly secret? Why or why not? Hint: check whether posteriori probabilities are equal to priori probabilities.

5. **Entropy**

   Based on the distributions in Figure 1, how much information about the key will leak if one ciphertext is revealed? What are the ideal values for H(P), H(K), and H(C)? Justify your answer.



$\Pr[P|a] = 0$

$\Pr[P|b] = 0$

$\Pr[P|c] = 1$

$\Pr[Q|a] = \Pr[k_2] = ¼$

$\Pr[Q|b] = \Pr[k_1] = ¾$

$\Pr[Q|c] = 0$

$\Pr[R|a] = \Pr[k_1] = ¾$

$\Pr[R|b] = \Pr[k_2] = ¼$

$\Pr[R|c] = 0$

| keyspace |
|---|
| $\Pr[\mathbf{K}=k_1] = ¾$ |
| $\Pr[\mathbf{K}=k_2] = ¼$ |

Figure 1: Plaintext, Ciphertext, and Key Distributions of a Cryptosystem

6. **Unicity Distance**
   Compute the Unicity distances of Permutation Cipher (block size=6). Compare its security with Substitution Cipher.

7. **Unicity Distance**
   Based on the letter frequency of Dutch language in Table 1, how many ciphertext characters does an attacker need to break the substitution cipher?

Table 1: Character Frequency: Nederlands (Dutch)

| Character | Frequency % | Character | Frequency % | Character | Frequency % |
|---|---|---|---|---|---|
| E | 19,06 | G | 3,12 | C | 1,30 |
| N | 9,91 | K | 2,79 | F | 0,73 |
| A | 7,66 | M | 2,56 | Y | 0,06 |
| T | 6,42 | V | 2,24 | X | 0,05 |
| I | 6,29 | U | 2,10 | Ë | 0,03 |
| O | 5,80 | J | 1,82 | Ä | 0,03 |
| R | 5,62 | W | 1,72 | Ü | 0,02 |
| D | 5,41 | Z | 1,60 | Q | 0,01 |
| S | 3,84 | P | 1,49 | Ö | 0,01 |
| L | 3,80 | B | 1,36 | Ï | 0,01 |
| H | 3,12 | | | | |

8. **Redundancy and Ciphertexts**
   Compute the redundancy of Dutch language. Let us assume we have a Dutch text file of around 10 MB, how much will be the size after the compression?

9. **Redundancy and Ciphertexts**
   Compare the security of Dutch and English languages in terms of redundancy.

# Practice Session 3

## Defining Security

## Security and Cryptography (CS4520)

1. **Stream Cipher**

   A company in Amsterdam uses a state of the art IND-CPA secure encryption scheme. The plaintext they encrypt are of the form ”yes” or ”no”. They are careful in keeping the secret key, following correct encryption procedures and not revealing the outcome of any decryptions.

   Upon entering an important negotiation, they are surprised to discover that their competitor in Delft already knows in advance their decision to go ahead or cancel a project.

   - How did the company misinterpret IND-CPA security?
   - What can they do to fix the problem?

2. **Security games**

   Consider the indistinguishable notion of security (IND).

   1. In a security game between an adversary and a challenger where the challenger selects the messages, explain the major difference(s) between an IND-CPA security game and an IND-CCA security game for a symmetric encryption scheme.
   2. In simulating a security game between an adversary and a challenger using an IND-CPA secure scheme, simulate a security game for the case where the adversary selects 5 messages $\{m_0, m_1, m_2, m_3, m_4\}$ to play the game. Using probability, provide the advantage of the adversary. Also provide the advantage for the general case (distinguishing between one of $n$ messages).
   3. Draw the security game described in (2). Assume a symmetric encryption scheme.

3. **Discrete Logarithm Problem**

   As you have learned, the RSA problem is a trapdoor one-way function. Is DLP (see book §3.1) a one-way function? And is it also a trapdoor one-way function? Explain your answer.

4. **PRG strategies**

   Consider the following functions $f : \{0,1\}^2 \rightarrow \{0,1\}^3$ and $g : \{0,1\}^2 \rightarrow \{0,1\}^3$ that are defined by $f(s_1, s_2) = (s_1, s_1 \oplus s_2, s_2)$ and $g(s_1, s_2) = (\overline{s_1}, \overline{s_2}, 0)$.[1] The class $\mathcal{T}$ consists of the algorithms $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ described in Table 2.

   Consider a candidate pseudorandom number generator PRG. Define the advantage of an *Adversary* against PRG as:

$$\text{Advantage}_{\text{PRG},\mathit{Adversary}} = \left|Pr\left[r \leftarrow \{0,1\}^3 : \mathit{Adversary}(r) = 1\right] - Pr\left[s \leftarrow 0, 1^2; r = \text{PRG}(s) : \mathit{Adversary}(r) = 1\right]\right| \tag{1}$$

[1] The $\oplus$-sign indicates the XOR-operation, $\overline{b}$ indicates the inverse of $b$.

| $\mathcal{A}(r_1, r_2, r_3)$ | $\mathcal{B}(r_1, r_2, r_3)$ | $\mathcal{C}(r_1, r_2, r_3)$ |
|---|---|---|
| Return $r_1 \oplus r_2$ | If $r_1 = 0$ return $r_2$ | $b_1, b_2 \leftarrow \{0, 1\}$ |
|  | else return $r_3$ | If $b_1 = b_2 = 0$ return 1 |
|  |  | else return 0 |

Table 2: Adversarial strategies $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$.

1. Compute Advantage$_{\mathcal{A},f}$, Advantage$_{\mathcal{B},f}$, Advantage$_{\mathcal{C},f}$, Advantage$_{\mathcal{A},g}$, Advantage$_{\mathcal{B},g}$, Advantage$_{\mathcal{C},g}$.
2. Describe an adversary $\mathcal{D}$ who will have a non-negligible advantage over both $f$ and $g$. Clearly provide the advantage in each case.
3. Given a pseudorandom generator $G : \{0,1\}^n \rightarrow \{0,1\}^{n+1}$, define $G' : \{0,1\}^n \rightarrow \{0,1\}^{2n+1}$ as $G'(s) = G(s)||1^n$. Provide a proof arguing that $G'$ is secure or insecure.[2] (Describe an adversary and provide the advantage using probability.)

[2] Note that $a||b$ indicates the concatenation of $a$ and $b$.

# Practice Session 4

## Modern Stream Ciphers

## Security and Cryptography (CS4520)

1. **Modern Stream Cipher**

   (a) *(0 points)* Assume a degree-6 LFSR with $c_1 = c_6 = 1$ and $c_2 = c_3 = c_4 = c_5 = 0$ .

   - What are the first 10 bits output by this LFSR if it starts in initial state of all ones?
   - Is this LFSR maximal length?

   (b) *(0 points)* Assume an 8-degree LFSR with $c_2 = c_3 = c_4 = c_8 = 1$ and $c_1 = c_5 = c_6 = c_7 = 0$.

   - What are the first 20 bits output of the LFSR with initial state $(s_7, \ldots, s_0) = (0, 1, 0, 1, 0, 1, 0, 1)$?
   - Is the LFSR maximal length? Explain your reasoning.

   (c) *(0 points)* Let $B : \ldots, b_{-1}, b_0, b_1, \ldots, b_i, \ldots$ be a bit sequence, i.e. $b_i \in \{0, 1\}$, such that $b_i = b_{i+5}$ and $b_i = b_{i+7}$ for all $i$. Show that $B$ is a constant sequence, in other words $b_i = b_j$ for all $i, j$.

   If a bit sequence $B$ satisfies $b_i = b_{i+M}$ and $b_i = b_{i+N}$ for all $i$, then show that $b_i = b_{i+d}$ where $d = gcd(M, N)$.

# Practice Session 5

## Block Ciphers and Modes of Operation, Hash Functions, MAC, and Key Derivation Functions

## Security and Cryptography (CS4520)

1. **Block Cipher and Modes of Operation**

   (a) *(0 points)* Explain in your own words what a mode of operation is.

   (b) *(0 points)* Explain what Electronic Code Book mode is and why it does not give an IND-CPA secure private-key encryption scheme.

   (c) *(0 points)* In Cipher Block Chaining mode, we use a block cipher

   $$F : \{0,1\}^n \times \{0,1\}^l \to \{0,1\}^l$$

   to construct a private-key cryptosystem for arbitrary length messages as follows. The key is a randomly chosen $k \leftarrow \{0,1\}^n$ . To encrypt a message $m = (m_1, \ldots, m_N)$ , where $m_1, \ldots, m_N \in 0, 1^l$ we pick a random IV $\leftarrow \{0,1\}^l$ , define $c_0 =$ IV, and compute $c_1, \ldots, c_N$ as $c_i = F_k(m_i \oplus c_{i-1})$ . The ciphertext is $c = (c_0, \ldots, c_N)$ . Specify the corresponding decryption algorithm.

   (d) *(0 points)* Consider AES in the following mode of operation: To encrypt an $l-$block message $M = (M_1, \ldots, M_l)$ using a 128-bit key $K$ we compute the ciphertext $C = (C_1, \ldots, C_l)$ by setting $C_1 = M_1 \oplus AES_K(0^{128})$ and for $i \geq 2$ setting $C_i = M_i \oplus AES_K(C_{i-1})$ . Is this mode of operation IND-CPA secure? Argue why or why not.

2. **Message Authenticating Codes**

   (a) *(0 points)* Consider the following one-time message authentication code for 10-bit messages.

   **Key generation:** The secret key is $sk = (a\ , b)$ , where $a\ , b \leftarrow \mathbb{Z}_{1031}$ are picked are random. (1031 is a prime).

   **Authentication:** To authenticate a message $m$, compute the message authentication code $t = am + b \bmod 1031$ .

   **Verification:** To verify a message authentication code $t$ on a message $m$, check whether $t = am + b \bmod 1031$ .

   Consider an adversary that does not know anything about the secret key, but does learn one pair $(m, t)$ of an arbitrary message and its corresponding message authentication code. What is the probability that the adversary can find a different message $m'$ and its corresponding message authentication code $t'$?

   (b) *(0 points)* Consider the following message authentication code for 128-bit messages built from the AES encryption function $E$ .

   **Key generation:** Pick a 128-bit secret key $k$ .

   **Authentication:** Given a message $m$ compute the message authentication code as $t = E_k(m)$ .

**Verification:** To verify a message authentication code t on a message $m$ , check whether $t = E_k(m)$ .

Assume $E_k$ were a truly random permutation of 128-bit strings. Suppose the adversary learns pairs of messages and message authentication codes $(m_1, t_1), \ldots,$ $(m_{1024}, t_{1024})$ for 1024 different messages of its own choosing. What is the probability that he can find a new message $m \notin \{m_1, \ldots, m_{1024}\}$ and guess the corresponding message authentication code $t$?

(c) *(0 points)* Recall that NMAC and HMAC are message authentication codes built from a Merkle-Damgard type hash-function such as for instance SHA-256. HMAC computes the message authentication code as HMAC$(k\ , m) = H(k \oplus opad\ , H(k \oplus ipad))$ , whereas NMAC computes the message authentication code as NMAC $(k\ , m) = H_{K_1}(H_{k_2}(m))$ with $k = (k_1\ , k_2)$ . Name an advantage of NMAC over HMAC and an advantage of HMAC over NMAC?

(d) *(0 points)* Let $F$ be a pseudorandom function. Show that each of the following MACs is insecure, even if used to authenticate fixed-length messages. (In each case **Key generation** outputs a uniform $k \in \{0\ , 1\}^n$ . Let $\langle i \rangle$ denote an $n/2$-bit encoding of the inteer $i$ .

1. To authenticate a message $m = m_1\ , \ldots\ , m_l$ , where $m_i\ , \in \{0\ , 1\}^n$ , compute $t := F_k(m_1) \oplus \ldots \oplus F_k(m_l)$ .
2. To authenticate a message $m = m_1\ , \ldots\ , m_l$ , where $m_i\ , \in \{0\ , 1\}^{n/2}$ , compute $t := F_k(\langle 1 \rangle || m_1) \oplus \ldots \oplus F_k(\langle l \rangle || m_l)$ .
3. To authenticate a message $m = m_1\ , \ldots\ , m_l$ , where $m_i\ , \in \{0\ , 1\}^{n/2}$ , choose uniform $r \leftarrow \{0\ , 1\}^n$ , compute $t := F_k(r) \oplus F_k(\langle 1 \rangle || m_1) \oplus \ldots \oplus F_k(\langle l \rangle || m_l)$ , and let the tag be $\langle r\ , t \rangle$ .

3. **Hash Functions**

(a) *(0 points)* In this part, we consider hash functions $H : \{0\ , 1\}^* \rightarrow \{0\ , 1\}^n$ .

Describe in your own words, the following terms pre-image attack, second pre-image attack, and collision attack.

(b) *(0 points)* Explain what a birthday attack is and how it works.

# Practice Session 6

## Public Key Encryption and Signature Algorithms
## Security and Cryptography (CS4520)

1. **Public Key Encryption & Signatures**

   (a) Explain the Decisional Diffie-Hellman, Discrete log and Computational Diffie-Hellman assumptions and show their relationship.

   (b) You are provided with a crypto-scheme X described bellow, answer the following questions.

   Let $\mathcal{N} = p \cdot q$, where $p, q$ are primes. Assume $\mathcal{G}$ is the cyclic group of modulo $\mathcal{N}^2$. $a$ and $\alpha$ are two random numbers in $\mathcal{Z}^*_{\mathcal{N}^2}$. Then, set $g = \alpha^2 \; mod \, \mathcal{N}^2$ and $h = g^a \; mod \, \mathcal{N}^2$. Now, the public key is $(N, g, h)$ and the secret key is $a$.

   To encrypt a message $m \in \mathcal{Z}_N$, a random number $r \in \mathcal{Z}_{\mathcal{N}^2}$ is chosen and the ciphertext $(A, B)$ is computed as

   $$A = g^r \; mod \, \mathcal{N}^2 \qquad\qquad B = h^r \cdot (1 + m\mathcal{N}) \; mod \, \mathcal{N}^2$$

   Analyze the security of X against OW/IND-CPA and OW/IND-CCA attacks based on the security games.

   (c) To obtain a signature $s$ of a message $m$ using RSA-FDH, with the private key $(n, d)$ the following operation is performed:

   $$s = H(m)^d \;\; mod \; n$$

   Assume the hash function $H(\cdot)$ is not cryptographically secure and an attacker has the following information:

   - Attacker has four messages $m$, $m_1$, $m_2$, and $m_3$ and their corresponding hash values, where the hash values are related as bellow:

     $$H(m_1) = 256 \cdot H(m_2) \quad H(m) = 256 \cdot H(m_3)$$

   - The attacker can call the signature function to get signatures of $H(m_1)$, $H(m_2)$, and $H(m_3)$.

   Show how an attacker can forge a signature for the message $m$.

   (d) Explain the Digital Signature Algorithm. Show that using the same ephemeral key $k$ leaks the private key $x$.

# Practice Session 7

## Certificates, Key Transport, and Key Agreement

## Security and Cryptography (CS4520)

1. **Certificates and Key Agreement**

   (a) Consider the following modified version of Needham-Shroeder protocol (similar to the Protocol Version 2 in the book):

   - $A \to S : A, B, N_A$
   - $S \to A : \{K_{ab}, N_A\}_{K_{bs}}, \{K_{ab}, N_A\}_{K_{as}}$
   - $A \to B : \{K_{ab}, N_A\}_{K_{bs}}, A$
   - $B \to A : \{N_A - 1\}_{K_{ab}}$

   Show that the protocol is not secure.

   (b) Consider the Needham-Shroeder Protocol given below. Explain what $N_a$ and $N_b$ are and their use in the protocol.

   - $A \to S : A, B, N_a$ ,
   - $S \to A : \{N_a, B, K_{ab}, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$,
   - $A \to B : \{K_{ab}, A\}_{K_{bs}}$,
   - $B \to A : \{N_b\}_{K_{ab}}$,
   - $A \to B : \{N_b - 1\}_{K_{ab}}$

   (c) Explain the Diffie-Hellman key exchange protocol and deploy the man-in-the-middle attack.

   Also, explain a solution against the man-in-the-middle attack for the DH key exchange protocol.

   (d) Alice and Bob would like to create a shared key using the Elliptic Curve version of the Diffie-Hellman key exchange protocol. Provide the domain parameters and the protocol.

# Practice Session 8

## Secret Sharing

## Security and Cryptography (CS4520)

1. **Secret Sharing**

   (a) Consider a $(5,5)$-threshold secret sharing over $\mathbb{Z}_{19}$ with a secret $s = 11$. Compute the shares of A, B, C, D, and E. Show how they all can reconstruct the secret.

   (b) Given the polynomial $P(x) = 3x^2 + 6x + 7 \bmod 11$, five parties, A, B, C, D and E, would like to participate in a $(t,n)$-threshold secret sharing scheme. The following set of users can obtain the secret:

   1. A and B
   2. B and C
   3. A, C and D
   4. D, C, and E.

   Answer the following questions:

   - What is the secret?
   - What is the minimum value of $t$?
   - Determine the number of shares for each party and produce those shares: $s_1, s_2, s_3, \ldots, s_n$.

   (c) Let 128-bit secrets $S_1, S_2 \in \mathbb{Z}_p$ be shared between $n$ participants using Shamir's SSS. The dealer wants to share a third secret $S_3$ such that $S_3 = 5 \times S_2 + S_1 \bmod p$. Other than standard sharing procedure of $S_3$, is there an efficient way? Explain.

   (d) *Idealness* of a secret sharing scheme (SSS) is a notion related with the proportion of the secret size over the share size. In order to give a formal definition, *information rate* can be defined as

   $$\rho = \min_{i \in \{1,\ldots,n\}} \frac{\log |\mathcal{S}|}{\log |\mathcal{S}_i|}$$

   where $\mathcal{S}$ and $\mathcal{S}_i$ represent the sets of all possible values for the secret and $i^{th}$ share, respectively. A SSS is *ideal* if and only if $\rho = 1$, i.e., with information rate equal to 1.

   Is Shamir's SSS an ideal one? Compute the information rate of Shamir's SSS.