UNIVERSITY OF BIRMINGHAM

School of Computer Science

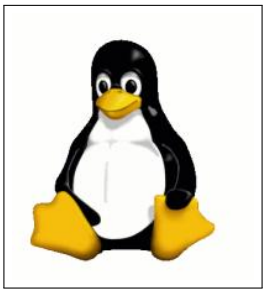
Network Security and Cryptography

Main Summer Examinations 2022

Network Security and Cryptography

Question 1 (Symmetric-key cryptography)

Consider the following 196 x 216 image, and imagine that the image is stored in raster format as follows: (r_i, g_i, b_i) are the red, green and blue values of the ith pixel, and they are in the range 0 to 255. The image is stored as a file with the following sequence of bytes: $r_1, g_1, b_1, r_2, g_2, b_2, \ldots r_{42336}, g_{42336}, b_{42336}$.



(a) The file is encrypted using AES-128 in ECB mode. Explain why the outline of the penguin will be visible in the encrypted file. **[5 marks]**

Let M1-ECB mode be the following modification of ECB mode:

- ctr_i is defined as the 128 bits obtained by writing the number i in binary notation, with the appropriate number of leading zeros to make 128 bits. (If $i > 2^{128} - 1$ then ctr is not defined.)
- The plaintext is split into blocks $p_1, p_2, \ldots, p_n$, each of size 128 bits (the last block is padded with zeros if necessary).
- The ith ciphertext block c_i is obtained by encrypting the result of ctr_i XOR'd with p_i. In symbols:

$$c_i = \mathsf{Enc}(ctr_i \oplus p_i)$$

where Enc is raw AES-128 encryption. The ciphertext consists of the ciphertext blocks $c_1, \ldots, c_n$.

(b) The original file of the penguin is now encrypted using AES-128 in M1-ECB mode. Is the outline of the penguin visible in the encrypted file? Explain your answer. **[5 marks]**

Consider now M2-ECB mode, which is the following modification of ECB mode:

- A 128-bit nonce r is chosen uniformly at random.
- The plaintext is split into blocks $p_1, p_2, \ldots, p_n$, each of size 128 bits (the last block is padded with zeros if necessary).

- The ith ciphertext block c_i is obtained by encrypting the result of r XOR'd with p_i. In symbols:

$$c_i = \mathsf{Enc}(r \oplus p_i)$$

where Enc is raw AES-128 encryption. The ciphertext consists of the nonce r together with the ciphertext blocks $c_1, \ldots, c_n$.

(c) The original file of the penguin is now encrypted using AES-128 in M2-ECB mode. Is the outline of the penguin visible in the encrypted file? Explain your answer. **[5 marks]**

(d) Does M2-ECB satisfy IND-CPA? Explain your answer. If your answer is "yes", your explanation should include a detailed intuition as to why it is "yes". If your answer is "no", your explanation should consist of a strategy for the attacker to win the game with probability significantly greater than 0.5. **[5 marks]**

Question 2 (Public-key cryptography)

Consider the following variation of the Schnorr digital signature scheme that we will call SchnorrPlus.

- KG(λ):
  - Randomly choose primes p and q such that q divides $p-1$ and where q is the order of a subgroup $G_q = \langle g \rangle$ of $\mathbf{Z}_p^\star$ where the Discrete Log problem is hard to solve
  - Choose $H : \{0,1\}^\star \to \mathbf{Z}_q$ a hash function
  - Define a secret value sec uniformly at random from $\{0,1\}^{256}$
  - Compute $y = g^x \bmod p$ where $x = H(\text{sec})$
  - Publish the public key $vk = (p, q, g, y, H)$
  - Retain the private key $sk = \text{sec} \in \{0,1\}^{256}$
- Sign(sk, M):
  - Compute $r = H(sk, M)$
  - Compute $s = H(M, g^r)$
  - Compute $x = H(sk)$
  - Compute $t = (r + x \cdot s) \mod q$
  - Output signature $\sigma = (s, t)$
- Verify(vk, σ, m):
  - Parse σ as (s, t)
  - Accept the signature if $H(M, g^t y^{-s}) = s$
  - Otherwise reject the signature

(a) Show that the SchnorrPlus signature scheme is correct, namely that for any message $M \in \{0,1\}^\star$ running Verify$\big(vk, \text{Sign}(sk, M), M\big)$ outputs accept if $(vk, sk) \leftarrow \text{KG}(\lambda)$. **[5 marks]**

(b) Can a signature scheme with a deterministic signing algorithm be secure against existential forgery attacks? Justify your answer. **[5 marks]**

The exam paper continues on the next page.

(c) Let M and M' be two *different* bit strings. Consider the following quantities:

$$\hat{r} = H(sk, M') \qquad \text{(notice } M' \text{ is used here)}$$
$$\hat{s} = H(M, g^{\hat{r}}) \qquad \text{(notice } M \text{ is used here)}$$
$$x = H(sk)$$
$$\hat{t} = (\hat{r} + x \cdot \hat{s}) \mod q$$

Let us define $\hat{\sigma} = (\hat{s}, \hat{t})$. What is the output of Verify$(vk, \hat{\sigma}, M)$ where $(vk, sk) \leftarrow$ KG(λ)? Justify your answer. **[5 marks]**

(d) Given your answers to the previous questions, do you think the signature scheme SchnorrPlus is *insecure* against existential forgery attacks? Justify your answer. **[5 marks]**

Question 3 (Network security)

You are approached by a major news outlet, which often communicates with whistleblowers. The news outlet wants you to give recommendations on how whistleblowers can communicate with them anonymously and securely. The whistleblowers are concerned about (i) someone tracing the information back to their real identities (**anonymity** of the whistleblower), (ii) someone other than the news outlet getting access to the communications (**confidentiality**), and (iii) someone modifying the content of the communications (**data integrity**).

The usual mode of communication is via email.

(a) Can encrypted email be used to achieve the desired properties for both parties (the whistleblower and the journalist)? Advise the parties on how to deploy S/MIME and/or PGP for this purpose, paying attention to encryption, signing, key management, and key authentication. Justify your answers in relation to the goals mentioned above (anonymity, confidentiality, data integrity). **[6 marks]**

(b) Would you recommend to use any other email security standards to achieve these goals (STARTTLS, SPF, DKIM, DMARC)? Justify your answer in relation to the goals. **[4 marks]**

Some of the whistleblowers feel uncomfortable to send the emails via their internet connections at home. Instead, they visit a shop in a busy city centre that offers free Wi-Fi. They connect to a web email provider via HTTPS (using a secure cipher suite) and send the emails from there. Consider the following scenarios and actors:

S1: An open Wi-Fi hotspot, no use of VPN/Tor. Actors: adversary monitoring wireless network traffic, access point provider.

S2: An open Wi-Fi hotspot, and also use of a VPN provider. Actors: adversary monitoring wireless network traffic, access point provider, VPN provider.

S3: An open Wi-Fi hotspot, and also use of Tor. Actors: adversary monitoring wireless network traffic, access point provider, Tor nodes.

S4: A WPA3 secured Wi-Fi hotspot, no use of VPN/Tor. Actors: adversary monitoring wireless network traffic, access point provider.

(c) For each scenario and actor, briefly describe what the actor might learn about the whistleblowers' connection with the webmail server (nothing, existence of connection, contents of communication). Also explain why the actor can learn this information and not more. **[8 marks]**

(d) One person proposes to use Apple's iMessage service instead of emails. Would you support this suggestion? Explain your answer and relate it to the goals above. **[2 marks]**