Problems and Solutions for Chapter 17

1. Consider a replacement of a paper-based ticketing system with an RFID system for a public transport system. What are benefits and drawbacks for the service provider ? What are benefits and drawbacks from a customer perspective ?

   Solution:
   Benefits for the provider include the following ones:

   - Personal costs for service operation can be reduced due to more automated controls.
   - Failures for reading tickets are reduced because RFID tickets are more resistant to stress (humidity, mechanical bending, and torsion) and data quality does not depend on printer cartridges.
   - Failures due to the choice of wrong tickets by the customers are minimized as the ticket costs can be automatically computed at the exit gate. This gives the customer more flexibility and allows a quick check-in to the transport service.
   - RFID technology is a new technology that can improve the corporate image.
   - RFID technology prevents existing fraud attacks due to forgery of paper tickets.
   - RFID technology enables options for a more refined use of automated physical control gates in the traffic system.
   - RFID technology enables a detailed analysis of customers' usage of the service (entry gate, exit gate, time of travel, frequency of system use).
   - A detailed analysis of data collected by an RFID system helps to continuously improve the service.

   Drawbacks for the provider include the following ones:

   - The development of an RFID system causes costs for the RFID infrastructure and usually additional costs for services by a system integrator.
   - The operation of an RFID system causes costs for maintenance.
   - The analysis of customer complaints can become complicated.
   - The provider has usually limited capabilities to assure the achieved security strength of the implemented RFID system. Usually, the provider has to trust the manufacturers, system integrators, or third parties.
   - Security or privacy incidents of the implemented RFID system can impair the corporate image.

   Benefits for the customer include the following ones:

   - Failures for reading tickets are reduced because RFID tickets are more resistant to stress (humidity, mechanical bending, and torsion) and data quality does not depend on printer cartridges.
   - Failures due to the choice of wrong tickets by the customers are minimized as the ticket costs can be automatically computed at the exit gate. This gives the customer more flexibility and allows a quick check-in to the transport service.

- A detailed analysis of data collected by an RFID system helps to continuously improve the service.

Drawbacks for the customer include the following ones:

- The customer looses control in a complex RFID system. It can be difficult to verify the ticket data, e.g., only at special machines. It can be difficult for the customer to gain evidences in case of complaints about the service, the pricing, or possible fraud.
- The customer looses privacy in the transport system, and possibly also outside the transport system. The customer looses control on personal movement data. The customer depends on the security and privacy of the implemented RFID system and on the trustworthy handling of sensitive information by the provider.
- The customer may feel victimized, restricted, educated or exposed by the automated RFID system.

2. What is the primary threat for an RFID based payment scheme in a canteen that uses

   (i) RFID tags without any cryptographic function (low-end RFID system),
   (ii) RFID tags with general-purpose cryptographic functions (mid-range RFID system).

   For both cases, design appropriate security functions.

   Solution: The primary threat is identical for both cases: RFID-enabled theft of assets. More concretely, the adversary aims at getting the meal without paying. Technically, this kind of fraud can be due to a replay attack, a relay attack, or due to cloning of RFID transponders.

   (i) RFID tags without any cryptographic function (low-end RFID system): The RFID tags do have a permanent ID, but no cryptographic function. Because of that, replay as well as cloning cannot be prevented by the RFID transponder and RFID reader. The security functions have to be implemented in the back-end. Typically, security functions consists of shadow accounts and blacklisting. At the time of transaction, an online connection is required to the back-end system and the black list and shadow account have to be checked. For the prevention of relay attack, the cashier should check that the customer holds an original transponder without any additional electronics to the RFID reader.
   (ii) RFID tags with general-purpose cryptographic functions (mid-range RFID system). Security functions can be implemented in the RFID transponder and RFID reader. Often cryptographic protocols with random numbers (so called “challenge-response” protocols) are used in order to provide access control to the tag data and to assure confidentiality of the transaction on the radio interface. The random numbers aim at preventing a replay attack. Security functions in the back-end system are not necessary, but may support the detection of fraud due to exploited vulnerabilities in the RFID system. For the prevention of relay attack, the cashier should check that the customer holds an original RFID transponder without any additional electronics to the RFID reader.

3. Summarize advantages and disadvantages for the privacy approaches “Killing Scheme”, “On-Tag Scheme”, “Agent Scheme”, and “User Scheme”. For this task, consider the achieved privacy solution, its user-friendliness, after-sales applications, and the required costs of implementing this functionality.

   Solution:

Scheme	Privacy Solution	User-friendliness	After-Sales Applications	Implementation Costs
Killing Scheme	Effective	Good, nothing to do for the user.	Not possible	Almost no cost for the provider.
On-Tag Scheme	Depends on provider.	Good, nothing to do for the user.	Possible	Medium to high costs for the provider because of additional security functions in the RFID system.
Agent Scheme	Depends on user management of access control lists.	Difficult because of management complexity for the user.	Possible	High costs for the user because the user requires an agent, e.g., a smart phone with software for managing the tags.
User Scheme	Depends on the secure handling of the user password.	Difficult because of time consuming user authentication.	Possible	High costs for user or provider as a device for secure password entry is required.

4. Which clock frequency of the RFID reader is at minimum required in order to restrict the distance between a transponder and an RFID reader to fifteen metres in a distance bounding protocol ? Consider that the time for signal processing is negligible and that the reader precisely controls the timing of the transponder.

   Solution: The total distance of the signal round-trip is $\Delta r = 30\ m$. Light covers this distance in $\Delta t = \Delta r/c = 10^{-7} = 0.1\ \mu s$. A clock frequency of at least 10 MHz is needed for the RFID reader.

5. Should countermeasures against physical implementation attacks be required for RFID readers ?

Solution: Countermeasures against physical implementation attacks are also necessary for RFID readers. RFID readers are a more promising target of attack than RFID transponders if the RFID system uses a key derivation scheme and stores the master keys in the RFID reader. RFID readers are especially at risk if they are exposed in a public area.

6. Discuss why MIFARE Classic systems are still in wide use though its underlying cryptographic cipher CRYPTO1 is easy to break.

   Solution: The fraud because of the break of CRYPTO1 is obviously negligible or still tolerable for many system providers.

7. How many years takes a brute-force attack on a cryptographic algorithm with a security strength of 80 bits, if special code breaking hardware would perform 50 billion crypto operations per second ?

   Solution: 2^{79} divided by $5 \cdot 10^{10}$ operations per second gives $1.2 \cdot 10^{13}$ seconds or $383,085$ years.

8. The following successive output bits of a Linear Feedback Shift Register (LFSR) of length 5 are given: $1,0,0,0,1,1,1,1,1,0$. Compute the feedback coefficients $c_1,\ldots,c_5$ and the subsequent output bits. What is the period of this LFSR ?

   Solution: The given output bits yield the following sequence of register states:

   $$\begin{array}{ccccc}
   1 & 0 & 0 & 0 & 1 \\
   1 & 1 & 0 & 0 & 0 \\
   1 & 1 & 1 & 0 & 0 \\
   1 & 1 & 1 & 1 & 0 \\
   1 & 1 & 1 & 1 & 1 \\
   0 & 1 & 1 & 1 & 1
   \end{array}$$

   This implies a system of linear equations (mod 2) for the feedback coefficients:

   $$\begin{array}{lll}
   c_1+ & c_5 & \equiv 1 \\
   c_1 + c_2 & & \equiv 1 \\
   c_1 + c_2 + c_3 & & \equiv 1 \\
   c_1 + c_2 + c_3 + c_4 & & \equiv 1 \\
   c_1 + c_2 + c_3 + c_4+ & c_5 & \equiv 0
   \end{array}$$

   The solution to this system of linear equations over the binary field is: $c_1 = 0$, $c_2 = 1$, $c_3 = 0$, $c_4 = 0$, $c_5 = 1$. The feedback bits after the given ten bits are: $0,1,1,0,1,0,0,1,0,0,0,0,1,0,1,0,1,1,1,0,1$ and then the output recurs. The period of the LFSR is 31.

9. Consider a linear congruential generator defined by $x_{n+1} \equiv ax_n + b \bmod m$ where a and b are secret parameters. The generator is initialized with a seed integer value x_0. Is this a cryptographically secure pseudo random number generator ?

   Solution: No, since three subsequent values x_n, x_{n+1}, x_{n+2} suffice to set up a 2 × 2 system of linear equations: $x_{n+2} \equiv ax_{n+1} + b \bmod m$ and $x_{n+1} \equiv ax_n + b \bmod m$. From this, the secret parameters a and b can be derived if $x_n \not\equiv x_{n+1} \bmod m$.

10. Assume that the keystream of a stream cipher recurs after some low period. What would be the consequence for the security of the cipher ?

    Solution: If the ciphertexts c_1 and c_2 are encrypted using the same keystream z, an adversary can compute the XOR of the corresponding plaintexts p_1 and p_2, which is a serious vulnerability: $c_1 \oplus c_2 = (p_1 \oplus z) \oplus (p_2 \oplus z) = p_1 \oplus p_2$.

11. What are the non-linear operations of the Trivium stream cipher ?

    Solution: The update of the each register involves an AND operation of the third- and second-last-bit of one of the other registers.

12. Many RFID tags are able to compute checksums (e.g. CRC16), defined by the remainder of a division over the polynomials of the binary field. Can such a *linear* function satisfy the requirements of a cryptographic hash function ?

    Solution: None of the requirements are satisfied. A preimage of any value y can be efficiently computed with some linear algebra. Since the values of a checksum (denoted by c) have a fixed bit-length, c can not be injective and $c(x) = 0$ for some easily computable value $x \neq 0$. Hence $c(x \oplus x') = c(x) \oplus c(x') = c(x')$ so that c is not second preimage resistant. This also implies that c is not collision resistant. Furthermore, the bit-length of a hash value should be at least 160 bits in order to resist collision attacks.

13. Why is it reasonable to use Elliptic Curve Cryptography for anti-counterfeiting protection in RFID systems ?

    Solution: A protected private key on the tag and a secure authentication protocol prevents spoofing, replay and cloning attacks. In principle, both symmetric and asymmetric cryptography can be used but the latter has advantages in distributed environments where the secure handling of symmetric keys can be very involved. Furthermore, Elliptic Curve Cryptography is feasible for transponders of moderate cost.