Selected Topics in Cryptography
Midterm Exam

23.5.2005

20th May 2005

- ⋆ The exam duration is 1h45’
- ⋆ All documents and electronic devices (except wireless communication devices) are allowed
- ⋆ For each question of every quiz, one and only one answer is correct
- ⋆ In every quiz, bad answers decrease the quiz grade
- ⋆ The final grade is based on the exercise and the 4 best quiz grades
- ⋆ If you do not enough space on the sheet, please use a separate page with your name one and clear references

LAST NAME: . . . .

First Name: . . . .

1 Quiz

1.1 Communication Security I-II

1. We can achieve secure communications over insecure channels by means of conventional cryptography provided that...

   □ DES is collision-resistant

   □ we have a secure channel at disposal

   □ we can rely on a trusted PKI

   □ we use SSL as a stream cipher

2. The number of rounds in AES can be...

   □ 128 □ 12 □ 64 □ 4×4

3. Using a stream cipher...

   □ the key can be used only once

   □ message integrity is strongly protected

   □ MD5 is more secure

   □ we can encrypt a single byte

4. Following the state of the art, what an adversary can *not* do against Bluetooth security?

   □ To decrypt packets on the fly.

   □ To prevent a radio packet from being received.

   □ To modify radio packets.

   □ To deduce a link key by listening to pairing and peer authentication protocols.

5. The Bluetooth pairing security is *not* improved by...

   □ using long PIN.

   □ running in a Faraday cage.

   □ frequent re-pairing by using the old link key as an init key.

   □ replacing E1, E21, E22 by better conventional cryptographic primitives.

1.2 Communication Security III-IV-V

1. We can sign digital documents by using

   □ Diffie-Hellman

   □ RSA-OAEP

   □ RSA-PSS

   □ SSL

2. X.509 certificates can authenticate public keys provided that...

   □ we can authenticate public keys.

   □ we avoid CBCPAD.

   □ we use `DH_anon` key exchange.

   □ RC4 is used.

3. Which of these problems does *not* apply to SSL?

   □ The master key can be limited to 40 bits for export from the US.

   □ Records are padded for CBC encryption after the MAC is computed.

   □ Users do not check unrecognized certificates.

   □ Users do not care which ciphersuite is accepted by their client.

4. By using a channel with special security assumptions *prior to any need for communications*, we would like to be able to set up secure communications over insecure channels. Which of the following assumptions is *not* sufficient?

   □ We can securely set up a symmetric key.

   □ We can securely set up a short password.

   □ We can authenticate a short string.

   □ We can authenticate a public key.

5. SAS-based authentication protocols can *not* be used...

   □ to rescue from key loss when running on the road

   □ to secure e-commerce

   □ to set up personal area networks

   □ to exchange PGP public keys

1.3 Codes and Cryptography

1. We consider a binary linear code defined by its generator matrix $\mathcal{G}$:

$$\mathcal{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

   A message m is transmitted over a binary symmetric channel with error probability 0.1 and the receiver gets $c = 0011111$. What is the most likely?

   □ $m = 001$.

   □ $m = 110$.

   □ $m = 1100$.

   □ $m = 0111$.

2. Which of these codes is *not* MDS?

   □ A Reed-Solomon code.

   □ A Goppa code.

   □ A repetition code.

   □ A $[17, 10, 8]$ code.

3. We compare the *encryption* speeds of AES, Niederreiter (with standard secure parameters) and RSA-1024. Which one is true?

   □ AES is faster than RSA which is faster than Niederreiter.

   □ RSA is faster than Niederreiter which is faster than AES.

   □ Niederreiter is faster than RSA which is faster than AES.

   □ AES is faster than Niederreiter which is faster than RSA.

4. Which of the following problems is proven to be NP-complete?

   □ Decoding in a random code.

   □ Decoding in a Goppa code.

   □ Distinguishing a scrambled Goppa generator matrix from a random matrix.

   □ Decoding in a scrambled Goppa code.

5. In the McEliece signature scheme, what is approximately the size of the public key?

   □ 80 bits.

   □ 150 bits.

   □ 65 536 bits.

   □ 9 Mbits.

1.4 RFID Security

1. Very cheap RFID tags which are used currently in supply chains (for example by Wal-Mart)...

   □ do not have antenna.
   □ contain asymmetric cryptographic functions.
   □ do not have their own power source.
   □ can communicate up to 250 meters.

2. Bono *et al.* have suggested an attack against the Digital Signature Transponder manufactured by Texas Instrument. Which of the following assertion is *false*?

   □ The key length used in this system is too short.
   □ The attacker can carry out an active attack by choosing the challenge to be sent to the tag.
   □ Bono *et al.* used a time-memory trade-off technique.
   □ The system is based on hash chains.

3. In current RFID protocols which can be proven to be secure (in terms of privacy), how many cryptographic operations are carried out by the system in order to identify the n tags it manages?

   □ $O(n)$.
   □ $O(n^2)$.
   □ $O(n^3)$.
   □ $O(n^4)$.

4. With protocols suited to very cheap tags, sensitive data should be exchanged over the Tag-to-Reader channel instead of the Reader-to-Tag channel, because...

   □ the Reader-to-Tag channel can be monitored from longer distances than the tag-to-reader channel.
   □ the Reader-to-Tag channel cannot be encrypted.
   □ it is easier for an attacker to access to a reader than to a tag.
   □ only the tag is tamper-resistant and thus can securely store sensitive data.

5. Which of the following sentences does *not* describe RFID tags?

   □ “If their cost reached 5 cents, they could be put on everyday lives items.”
   □ “They are already used to locate people in amusement parks.”
   □ “Their bearer can switch them off.”
   □ “Their communication range depends on the frequency they use.”

1.5 Undeniable Signatures

1. To ensure the security of an undeniable signature, . . .

   □ . . . the public key must be transmitted over a *confidential* and *authenticated* channel.

   □ . . . it is sufficient to send the public key over a *confidential* channel.

   □ . . . it is sufficient to send the public key over an *authenticated* channel.

   □ . . . no requirement about the security of the transmission channel of the public key is required.

2. Which of the following notion is *not* a security requirement of the denial protocol?

   □ completeness

   □ zero-knowledge

   □ invisibility

   □ soundness

3. Let G be a cyclic group generated by an element g. Let h be a given element of the group G. How many group homomorphisms $f : G \to G$ satisfy $f(g) = h$?

   □ 0 □ 1 □ 2 □ $\#G$

4. In the MOVA scheme, if the secret homomorphism is not uniquely defined by the public key. . .

   □ the signature generation is no more efficient.

   □ the signer is not able to sign anymore.

   □ the signer might be able to repudiate his signatures.

   □ the signer can prove the validity of the public key by running an additional interactive proof.

5. Which security notion prevents a signer from proving that a valid signature is invalid?

   □ zero-knowledge of the confirmation protocol

   □ soundness of the confirmation protocol

   □ soundness of the denial protocol

   □ zero-knowledge of the denial protocol

1.6 Password-Based Cryptography

1. The Bellovin-Merritt model requires...

   □ to authenticate a secret key.
   □ to authenticate a public key.
   □ to authenticate a secret password.
   □ a trusted third party.

2. EKE is...

   □ a password-based key agreement protocol based on Diffie-Hellman
   □ a protocol designed by Bellare and Rogaway
   □ a protocol the security of which was proven by Bellare, Pointcheval, and Rogaway
   □ a family of password-based key agreement protocols

3. Forward secrecy protects...

   □ the confidentiality of current communications in the future
   □ against offline dictionary attacks
   □ from running a protocol backwards
   □ the secrecy of long-term keys

4. Diffie-Hellman -based EKE protocols in which the first public key is sent in clear is vulnerable...

   □ when the challenges format includes redundancy
   □ when the challenges format includes no redundancy
   □ to *e*-residue attacks
   □ to random oracles

5. Given a subgroup G of prime order q of $\mathbf{Z}_p^*$ generated by some element g (where $p = 1 + qr$ is prime), which of the following mappings instantiates a full-domain symmetric encryption on G?

   □ $x \mapsto g^x \bmod p$
   □ $x \mapsto x \times H(w) \bmod p$ where H generates random strings
   □ $x \mapsto x \times H(w)^r \bmod p$ where H generates random strings
   □ $x \mapsto \mathsf{AES}_w(x) \bmod p$

2 Exercise

2.1 Cryptography for the Small

1. You are in Lausanne and you would like to securely communicate with your old friend in New York over the Internet, but you did not exchange any secret or public key in a reliable way yet. How can you initiate a secure communication by talking with your friend over the telephone?

   (Make your answer as precise as possible.)

2. In a network infrastructure, we would like to enable nodes to authenticate digital documents to everyone in a non-repudiable way and non-interactive way. For that, the document is attached to a single string *S*. We would like *S* to be verifiable in an offline way by anyone. Which cryptographic scheme can we use in order to make *S* have a length less than 200 bits?

↶

3. When the offline verifiability assumption is relaxed, how to achieve lengths less than 50 bits?

4. We would like to implement secure wireless communications with a hardware as cheap as possible. Which technology can we use for encryption? Which technology can we use for message authentication?

2.2 Yet Another Nightmare

We are in 2084, health insurance companies have taken control on the Swiss Federal Government. They have decided that every inhabitants should have RFID sensor implants to monitor health information of individuals, decide on appointments to be done with medical doctors, and of course, to adjust their insurance fees. Thanks to technologic advances, RFID tags can now implement strong cryptography. To simplify, we consider four tags per individuals:

- a sensor tag A (air) to measure what the individual breathes, smells, or smokes;
- a sensor tag B (blod) to measure cardiac activities, blod pressure, and the body temperature;
- a master tag C (collector) which collects information from other tags and talk to the insurance company through tag readers which are installed all around the country;
- a sensor tag D (diet) to measure which food arrives in the stomach for diet control.

We assume that all tags in the body have set up a long-term symmetric key so that they can securely communicate, that A, B, and D can only talk to C and not between them, that tags A, B, and D communicate only when there is anything new to tell C or when they are queried by C.

1. When eating a smelly cheese, diving, doing sport activities, and in many other situations, several tags may try to talk at the same time. Propose a protocol to solve this collision problem?

2. When a tag would like to send a message *x* to another tag, propose a cryptographic scheme so that the confidentiality of *x* is protected, as well as the authentication and the integrity.

3. We assume that inter-tag communication is secured by deterministic cryptographic schemes. In particular, when tag A detects a particular smell σ, it always sends the same message to tag C. The ground floor of department stores usually contains a lot of smells. How could a chain of department stores trace people? How to avoid it?

↷

4. We assume that tag C tries to upload a daily report of received messages to the insurance company. Based on that, the company may decide to arrange an appointment with a medical doctor, or charge a fine if the customer did not follow medical recommendations such as not to smoke, not to eat too fat, take (expensive) medicine, etc. Propose a security infrastructure so that reports are sent in a confidential, authenticated, and integer way to the company.

5. A group of cryptopunks have reverse engineered a few tags and designed a way to recover their long-term keys. How could they use it to divert the system on their own health insurance? How could they use it to make the system collapse?