Selected Topics in Cryptography
Final Exam

29th June 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, wrong answers *decrease* the survey grade
- ⋆ The final grade is based on the exercise grade and the 5 best quiz grades
- ⋆ If you have not enough space on the sheet, please use a separate page with your name on and clear references

LAST NAME: . . . .

First Name: . . . .

1 Quiz

1.1 Communication Security I-II

1. Galois Fields are *not* used in ...

   □ AES
   □ OMAC1
   □ SHA-1
   □ Elliptic curve schemes

2. Which of these acronyms is *not* related to CCM?

   □ MAC □ CBC □ OMAC □ CTR

3. Bluetooth packet authentication and integrity is ...

   □ protected by a CRC
   □ protected by the E4 primitive
   □ not protected
   □ protected by SAFER+

4. In Bluetooth, ...

   □ the link key can be of length one byte
   □ the encryption key can be of effective length one byte
   □ the unit key is used only once
   □ the init key is used for peer authentication

5. Dummy Bluetooth devices suffer from many security problems. Which of the following is *not* applicable.

   □ The PIN is a trivial constant.
   □ The encryption key is limited to 40 bits.
   □ The link key with any other device is forced to be a constant.
   □ The human operator has a limited interface.

1.2 Communication Security III-IV-V

1. Who plays with puzzles?

   □ Diffie

   □ Rivest

   □ Merkle

   □ ElGamal

2. The RSA public key cryptosystem requires...

   □ to generate private prime numbers.

   □ to factorize big numbers.

   □ to compute square roots in a multiplicative group.

   □ to set up a key by using the Diffie-Hellman protocol.

3. PKCS#1v1.5...

   □ includes a digital signature scheme with message recovery.

   □ includes variants of ElGamal signatures.

   □ is an IETF standard.

   □ is now obsolete.

4. Tick the *wrong* assertion.

   □ The SSL ciphersuites all use HMAC.

   □ The SSL ciphersuites specify how the master key is set up.

   □ MD5 and SHA-1 are always used in SSL handshakes.

   □ Encryption in SSL always use CBCPAD.

5. Tick the *wrong* assertion about the MANA I protocol.

   □ It can be used to authenticate long strings over insecure channels.

   □ It is based on a universal hash function.

   □ It can work with string as short as 20 bits.

   □ It is provably secure provided that we have an extra channel which can authenticate short strings at disposal.

1.3 Codes and Cryptography

1. A $[n,k,d]$ code denotes a code of length n, dimension k and minimal distance d. Which of these codes cannot exist?

   □ $[7,4,3]$.
   □ $[16,1,16]$.
   □ $[16,8,4]$.
   □ $[8,16,16]$.

2. In a $[n,k,d]$ code, we perform bounded decoding up to a distance t. At which condition is this decoding always unique?

   □ If $d > n-k+1$.
   □ If $t \leq n-k$.
   □ If $t \leq k$.
   □ If $t \leq \dfrac{d-1}{2}$.

3. In the McEliece cryptosystem, a message m is encrypted by computing $c = m \times \mathcal{G}' + e$. The matrix $\mathcal{G}'$ is the scrambled generator matrix of a Goppa code and is of the form $\mathcal{G}' = \mathcal{A} \times \mathcal{G} \times \mathcal{B}$. Which of the following assumptions is correct?

   □ $\mathcal{A}$ is a permutation matrix and $\mathcal{B}$ is invertible.
   □ $\mathcal{A}$ is invertible and $\mathcal{B}$ is invertible.
   □ $\mathcal{A}$ is invertible and $\mathcal{B}$ is a permutation matrix.
   □ $\mathcal{A}$ is invertible and $\mathcal{B}$ is singular.

4. The McEliece cryptosystem is said to suffer from a re-encryption problem. Which of these operations can be dangerous?

   □ Encoding two different messages with the same error.
   □ Encoding the same message with two completely different errors.
   □ Encoding two very similar messages (only a few bits of difference) with the same error.
   □ Encoding a same message with two different public keys.

5. We want to use an MDS matrix in the diffusion layer of a symmetric cipher. Its input is composed of p elements in GF(2^m) and it should output q elements in GF(2^m). Supposing we do not need any sub-block diffusion, what kind of code do we need to build if we want optimal diffusion?

   □ A $[q,p,q-p+1]$ code on GF(2^m).
   □ A $[mq,mp,m(q-p+1)]$ code on GF(2).
   □ A $[p+q,p,q+1]$ code on GF(2^m).
   □ A $[q,p,p+1]$ code on GF(2^m).

1.4 RFID Security

1. We consider the protocol of Ohkubo, Suzuki, and Kinoshita which is based on hash chains. Let G and H be two hash functions implemented within the tags, and let s be the secret initial value characterizing a given tag. In order to guarantee privacy, when the tag is queried during the ith identification, it should answer to the reader...

   □ $G(H(s))$.

   □ $G(H^i(s))$.

   □ $G^i(H(s))$.

   □ $G^i(H(s))||H^i(s)$.

2. Current adversarial models suited to RFID systems consider usually three kinds of channel from which an attacker may obtain information. Which of the following propositions is *not* relevant in this context?

   □ Backward channel.

   □ Forward channel.

   □ Memory channel.

   □ Secondary channel.

3. Why a cryptographically secure Pseudo-Random Number Generator should be implemented within the tag when the RFID system uses a collision avoidance protocol based on a time division e.g. slotted Aloha? Because...

   □ a given tag could be tracked according to its time slots distribution if it is biased.

   □ the tag uses a randomized encryption algorithm to answer to the reader.

   □ both reader and tag must have the same PRNG, initialized with the same value, in order to generate session keys.

   □ it is less expensive to implement a PRNG than a hash function.

4. We consider the following RFID protocol between a reader and a tag: the reader sends a nonce r, and the tag answers $\mathrm{AES}_s(r)$ where s is the identifier of the tag. Why such an RFID protocol should not be used? Because...

   □ this technique would allow an adversary to track the tags.

   □ tags are not able to use an encryption scheme due to lack of power.

   □ this technique would reveal the identifier of the tag.

   □ only the tags are able to initiate the protocol.

5. In RFID systems, collision avoidance protocols aim to...

   □ allow several tags to answer to a reader at the same time.

   □ allow a tag to communicate with several systems at the same time.

   □ allow one tag and one reader to transmit at the same frequency.

   □ allow several tags to communicate together.

1.5 Undeniable Signatures

1. Tick the *right* assertion.

   □ To convince a verifier that a message-signature pair (m,σ) is valid, the prover has to run the denial *and* the confirmation protocols.

   □ An undeniable signature scheme offers necessarily very short signatures.

   □ If the confirmation protocol fails on a given message-signature pair (m,σ), it implies that (m,σ) is invalid.

   □ The 2-move confirmation protocol of Chaum satisfies soundness even with a computationally unbounded prover.

2. Tick the commitment scheme which really exists (we have seen in the course!).

   □ Chaum commitment

   □ Pedersen commitment

   □ MOVA commitment

   □ Diffie-Hellman commitment

3. In a commitment scheme, which security notion prevents a cheating committer from changing his mind after having sent the committed value?

   □ completeness

   □ perfectly hiding

   □ non-repudiation

   □ computationally binding

4. Who invented the concept of undeniable signatures?

   □ Jean Monnerat and Serge Vaudenay

   □ Whitfield Diffie and Martin Hellman

   □ Torben Pedersen

   □ David Chaum and Hans van Antwerpen

5. Tick the *false* assertion.

   □ The Group Homomorphism Interpolation problem can be seen as a generalization of the Discrete Logarithm problem.

   □ An attacker who is able to solve the Group Homomorphism Interpolation Problem can forge some MOVA signatures.

   □ The prover does not need his secret key in the denial protocol of the MOVA scheme.

   □ The denial protocol of the MOVA scheme makes use of a commitment scheme.

1.6 Password-Based Cryptography

1. What is the most dangerous threat to classical challenge-response access control protocols?

   □ man-in-the-middle attacks

   □ online exhaustive search

   □ offline exhaustive search

   □ quantum computers

2. What is the advantage of the KOY protocol?

   □ It uses all symbols in the alphabet.

   □ It requires less computations than PAK.

   □ It requires less communications than PAK.

   □ It is provably secure without random oracles.

3. Which of these password-based key agreement protocols is based on RSA?

   □ SRP □ PEKEP □ PPK □ AuthA

4. The Bellovin-Merritt model for secure communications improves the conventional model in the sense that...

   □ we can use AES instead of DES

   □ every user relies on a specific public-private key pair

   □ the piece of information which has to be securely set up is shorter

   □ we no longer need confidential channels

5. Which of the following assertion is *not* a problem to design RSA-based password key agreement protocols?

   □ RSA moduli are easily distinguishable from random integers.

   □ RSA public exponents are likely to be coprime with 3.

   □ It is not easy to convince anyone that e is coprime with $\varphi(n)$ without disclosing the factorization of n.

   □ RSA requires precise formatting rules such as OAEP to be secure.

1.7 Identity-Based Cryptography

1. One problem with identity-based encryption is that...

   □ there are no secure schemes at this time.

   □ the authority can recover everyone's secret key.

   □ the public key is typically too large.

   □ it cannot work when someone has lost his ID card.

2. Pairing means...

   □ to have a private and a public key put together.

   □ to synchronize two Bluetooth devices.

   □ a bilinear mapping from an elliptic curve to a finite field.

   □ a group homomorphism form a cubic curve to paired rings.

3. Which of the following schemes is *not* an identity-based encryption scheme.

   □ Waters

   □ Boneh-Franklin

   □ Fujisaki-Okamoto

   □ Heng-Kurosawa

4. Assuming that we have a pairing $\hat{e} : G_1 \times G_1 \longrightarrow G_2$ given two cyclic groups G_1 and G_2 of given prime order q. We assume that G_2 is a subgroup of $\mathrm{GF}(p^2)^*$ where p is a given prime number and that G_1 is a subgroup of a supersingular elliptic curve over $\mathrm{GF}(p)$. Which of the following problems can be pretty hard?

   □ The decisional Diffie-Hellman problem in G_1.

   □ Finding a prime factor of the order of G_1.

   □ Computing the order of the elliptic curve.

   □ The discrete logarithm problem in G_1.

5. We assume that Alice wants to send a message to Bob using certificate-based encryption. Tick the *wrong* assertion.

   □ Bob has to get a certificate for his public key.

   □ Alice only needs the plaintext, Bob's and the authority's public keys to encrypt.

   □ Bob only needs the ciphertext and his secret key to decrypt the message.

   □ The certificate is frequently updated.

1.8 Broadcast Encryption and Traitor Tracing

1. We distinguish “stateless” and “stateful” broadcast encryption schemes. Stateless schemes...

   □ assume that the receivers have a low-bandwith return path to the broadcasting center.

   □ imply that the receivers can update parts of their secret information in case of emergency.

   □ do not fit into the model of PayTV decoders receiving the signal from a satellite.

   □ have a broadcast message length which depends on the number of revoked users.

2. The main difference between broadcast encryption schemes based on Complete-Subtree Cover (CSC) and Subset-Difference Cover (SDC) is that...

   □ schemes based on CSC are stateless while schemes based on SDC are stateful.

   □ SDC schemes do not take into account the Steiner tree built out of the revoked receivers.

   □ SDC schemes have a message complexity not depending on the total number of receivers.

   □ schemes based on CSC need clearly less key material to be stored on the receiver.

3. In the Boneh-Franklin traitor tracing scheme...

   □ a passive adversary able to break the semantic security can break the Decisional Diffie-Hellman Assumption.

   □ a passive adversary able to break the semantic security can break the Computational Diffie-Hellman Assumption.

   □ an active adversary able to break the semantic security can trivially factorize RSA moduli.

   □ a passive adversary able to mount a linear cryptanalysis against Reed-Solomon codes is able to trace revoked decoders.

4. When using the Boneh-Franklin traitor tracing scheme, coalitions of pirate having a size strictly smaller than the maximal allowed coalition size can...

   □ generate a single, untraceable new key able to decrypt the protected content.

   □ generate a large number of untraceable new keys able to decrypt the protected content.

   □ generate a single, traceable new key able to decrypt the protected content.

   □ generate a large number of traceable new keys able to decrypt the protected content.

5. We would like to implement the Boneh-Franklin scheme on a prime-order group. Let p and q be two prime numbers of respective size 1024 and 1023 bits such that $p = 2q+1$. Furthermore, let p' and q' be two prime numbers having a respective size of 1024 and 160 bits such that $p' = Nq'+1$ for some N. On the receiver side, it is more efficient to work...

   □ in the subgroup of order q in Z_p^* since both p and q have approximately the same size.

   □ in the subgroup of order q in Z_p^* since it is easier to find a generator of that subgroup.

   □ in the subgroup of order q' in $Z_{p'}^*$ since the modular exponentiations are done with 160-bit exponents.

   □ directly in the group Z_p^* (which has an order equal to $2q$), since it is not required to have a prime-order group to implement the Boneh-Franklin scheme.

2 Exercise

2.1 On Replacing Humans by Cryptography

Prologue: a telephone operator has fired 90% of its personnel and replaced call centers with web services. Now, customers have to go on the web over the Internet to manage their contract with the operator. This requires secure communications. The operator also removed paper-based mailings. Customers now receive invoices directly from their bank and announcements by email.

1. When a customer visits the operator's web site, how can he/she authenticate the operator?

2. Once a secure connection with the operator is established, the operator must authenticate the customer. Unfortunately, the restructuring was made in a rush and the operator did not provide any password nor any authenticating facilities to the customers.

   (a) Identify another usable communication channel between the customer and the telephone operator which can still provide some kind of security. In what follows we assume that this channel provides no confidentiality but authentication from the customer to the operator.

   (b) We now have two communication channels at disposal: the link A which provides secure communication in which the customer has authenticated the operator and the identified channel $B(\mathsf{ID})$ from the previous question which provides authentication from the customer of identity ID to the operator. We consider the following protocol.

Customer ID		Operator
	$\xrightarrow{A:\mathsf{ID}}$	receive ID', generate a password w
receive w'	$\xleftarrow{A:w}$	insert $(\mathsf{ID}', w, \mathsf{time})$ in a list L
	$\xrightarrow{B(\mathsf{ID}):\mathsf{ok}}$	receive ok from a channel $B(\mathsf{ID}'')$
		if there is a tuple (ID'', w'', t) in L
		with $t > \mathsf{time} - \Delta$, extract it
password: w'		and validate account (ID'', w'')

   In this protocol, time denotes the clock value and Δ denotes a maximum time delay after which a password request session expires on the server side if not completed. After the protocol completes, the customer can authenticate through the A link by using a password.

   Show how an adversary can mount an attack in which he/she can log in an account of identity ID.

(c) We fix the previous protocol by using a session identifier s as follows.

$$
\begin{array}{lcl}
\text{Customer } \mathsf{ID} & & \qquad\qquad \text{Operator} \\
 & & \text{increment a counter } s \\
 & \xrightarrow{\hspace{2cm} A:\mathsf{ID} \hspace{2cm}} & \text{receive } \mathsf{ID}', \text{ generate a password } w \\
\text{receive } s'||w' & \xleftarrow{\hspace{2cm} A:s||w \hspace{2cm}} & \text{insert } (s, \mathsf{ID}', w, \mathsf{time}) \text{ in a list } L \\
 & \xrightarrow{\hspace{2cm} B(\mathsf{ID}):s' \hspace{2cm}} & \text{receive } s'' \text{ from a channel } B(\mathsf{ID}'') \\
 & & \text{if there is a tuple } (s'', \mathsf{ID}'', w'', t) \text{ in } L \\
 & & \text{with } t > \mathsf{time} - \Delta, \text{ extract it} \\
\text{password: } w' & & \text{and validate account } (\mathsf{ID}'', w'')
\end{array}
$$

Show that if the account is validated and the customer of identity ID'' is honest, only this customer can have received the password w''.

3. The operator, which definitely has some liquidity problems, stops paying for certificates. How can we now launch secure communications over the Internet from a customer to the operator?

4. A malicious worm circulates and collects passwords of customers. Which action must be taken by the operator?

Epilogue: finally, the operator, which survived thanks to some financial support by the government, fired his cryptographers and launched a new call center in Asia.

2.2 ID Cards with Cryptographic Keys

The government would like to set up a public key infrastructure for every citizen. For this, some identity cards are given. We assume that ID cards have a tamper proof chip with a protected secret key inside and a scannable public key.

1. Assuming that the public key can be freely scanned by radio link, what is the threat for citizens?

2. We now assume that public keys are based on identity, i.e. there is a master public key which is common for every one and the citizen's public key is simply its name as it appears on the ID card. Secret keys are used to sign legal documents.

   Recall how secret keys are made. What is the major threat for citizens?

3. We now assume that the secret key is generated by the chip itself once it is switched on for the first time and that the public key is printed on the ID card and scannable by visual contact only. Again, the secret key is used to sign legal documents. More concretely, there is a button "sign" on the ID card. The chip receives the document to be signed by radio link, and if the button is pressed, the chip signs the document and sends the signature by radio link as well.

   (a) We assume that payments in shops are made by payment orders signed by the ID card. How can a shop overcharge a customer?

(b) We assume that payment orders are short messages and that there is now a display on the ID card which displays messages to be signed. Assume that vendors now always ask for the ID card for payments.

What is the threat for citizens?

4. We now assume that digital signatures are no longer used, but that identity-based encryption is implemented. Concretely, a message for a citizen can be encrypted by using the master public key and his/her identity as it displays on the card. The encrypted message can be sent to the chip on the ID card by radio link so that it can be decrypted by using the sealed secret key. The decrypted message is simply displayed on the card, but the card always remains silent on radio channels.

   Propose a scheme so that any organization can authenticate any citizen over the telephone.