Applied Cryptography, COMPGA12, 2009-10 **ANSWERS PAPER, CONFIDENTIAL**

Answer ALL questions. 2 hours.

Marks for each part of each question are indicated in square brackets

Calculators are NOT permitted

1. Multiple Choice Questions. For each question, out of four answers (a), (b), (c), (d), indicate which one is **incorrect**. In each question exactly 3 answers are correct and exactly one is incorrect.

1. Challenge-response authentication systems are dynamic, and secure against simple replay attacks. However, they are not secure against relay attacks, in which the whole communication between the authentic card and the genuine reader is relayed by the attacker, who tricks the reader into believing that the smart card chip is in the proximity of the reader. One can remark that:

   (a) Relay attacks are also at least equally possible, with traditional smart cards with electrical contacts (wired connection).

   (b) Communications of an electronic passport cannot be relayed over large distances, because the internal battery in the passport chip does not have enough power.

   (c) A method to protect an electronic passport's chip against being used without owner's consent and knowledge through a relay of communications, is to shield it electromagnetically (for example keep it in a closed metallic box, or in special wallet with aluminium foil embedded in the cover).

   (d) Another defence against relay attacks is to respond to queries very quickly and measure the time very precisely, given the fact that electromagnetic waves cannot travel faster than the speed of light.

[5 marks]

2. A smart card authenticates to the server in the following way: the server sends a 4 digit random number (a challenge), and the smart card responds to this challenge with a certain cryptogram (response) that depends on the random challenge. This type of dynamic authentication is called “challenge-response”. It is in principle secure against replay attacks, where the same cryptogram is replayed by the attacker at a later occasion. We can observe that:

   (a) The security breaks apart, if the server’s random number generator can be reset to its previous state or repeat some of the random numbers.

   (b) This is also a “mutual authentication system”, which authenticates both the card to the server, and the server to the card.

   (c) In this system, the challenge should not be very short (like 1 digit), otherwise the system is insecure.

   (d) To compute this cryptogram, we can use for example a MAC or a digital signature scheme.

[5 marks]

3. A SIM card found inside GSM mobile phones implements a challenge-response mechanism based on the key shared between the SIM card and the mobile phone operator. Best practice is to authenticate each individual phone call. The challenge should be different in each phone call and the smart card computes a suitable response cryptogram.

   (a) This cryptogram guarantees that the voice communication will be encrypted.

   (b) This is a dynamic authentication method, allows to prove that the right SIM card is present and alive.

   (c) The mobile phone and the base station (that can be in a different country) are just intermediaries in this process. They are not able to compromise the security of cryptographic keys stored in the SIM card.

   (d) If we insert our SIM card into our friend's phone and make a phone call, it is the owner of the SIM card that pays for the communication.

[5 marks]

4. A Pseudo-Random Number Generator (PRNG) is such that:

   (a) it is a deterministic algorithm, redoing it gives the same result

   (b) it is a probabilistic algorithm, the outcome is truly random,

   (c) it expands a short string of bits (seed) into a very long sequence of bits

   (d) the sequence of output bits should be indistinguishable from a source of really random, uniformly distributed and independent bits.

[5 marks]

5. When we “touch-in” or “touch-out” with the London Oyster card, some sort of authentication takes place before the reader is allowed to either read or write the data stored on the card.

    (a) The card first sends a password to authenticate the card to the reader, then the reader modifies an encrypted counter stored on the card. This password is a secret, different for each Oyster card.

    (b) When we use a London Oyster card, the terminal is cryptographically authenticated first, the card is authenticated second. Only in presence of a genuine reader, the card activates crypto functionalities that allow to prove it is genuine. The intention is to make it harder for hackers to attack a card that is in their possession, and makes the business of hacking the card harder and riskier for criminals. This is because they need to gain access to at least one legitimate reader, and it is usually available only at certain times, and at locations that can be closely monitored by CCTV and where all invalid authentication attempts will be recorded by the system.

    (c) The data within the card, such as our remaining credit, is encrypted during the transmissions between the card and the reader.

    (d) Every valid and functional Oyster card contains blocks of memory that cannot be modified, not even by the Transport for London chief system security officer.

[5 marks]

[Total 25 marks]

Solutions to 1.

1. b, there is no battery in e-passports

2. b, nothing authenticates the terminal

3. a, authentication; nothing to do with encryption

4. b, it is deterministic.

5. a, this would be insecure against replay attacks

2. Precise Questions to Answer. Brief answers will be appreciated.

1. Give a definition of a side-channel attack, does it break the cryptography, or is it about something else? Make your definition as general as possible.

   [5 marks]

2. Explain what is an SPA attack and some simple method to protect against it.

   [5 marks]

3. Explain how a DPA attack works.

   [5 marks]

4. Describe at least one defence method against DPA.

   [5 marks]

5. Why we would never use RSA to encrypt long messages? Explain the concepts of hybrid encryption, and the principles of data and key encapsulation.

   [5 marks]

6. Explain (in simple words) the concept of an Advanced Electronic Signature that exists in EU directives and is translated in the law of many countries. What are the main two broad and general security requirements that a 'good' electronic signature should satisfy?

   [5 marks]

7. Explain what data the MRZ (Machine Readable Zone) in an electronic passport contains. Why or how does it through the BAC (Basic Access Control) prevent a person sitting next to you in the London underground, from extracting your biometric data from the passport (i.e. from reading your RFID chip)?

   [5 marks]

8. Explain the most basic technique that is used by electronic passport to authenticate the data inside the passport. What is the name of the similar technique used in bank cards?

   [5 marks]

9. Which data groups in electronic passports are considered as very sensitive, so that a normal border checkpoint is NOT authorized to read them, but only an authorized "inspection system" that must be explicitly authorized by the issuing country?

[5 marks]

10. Explain how a smart card can protect PGP electronic email on a PC running Windows against malware.

[5 marks]

[Total 50 marks]

Quick Answers for 2.

1. A Side Channel Attack focuses on implementation of cryptography, and doesn't break cryptography, just the implementation (and defeats the overall practical ”physical” security of the device). Side channels are channels different than standard inputs and outputs of a cryptographic algorithm. The usage of such channels is not intended in the design of a secure cryptographic algorithm/protocol/system, but rather the consequence of the necessity to implement and use the cryptographic functionality in the real world. In a Side Channel Attack, the attacker is able to interact with a physical system that implements the cryptographic algorithm, and either some information will be leaked to the attacker, or he will be able to make some changes (perturbate) the device, and this will be exploited to compromise the security, for example to recover the secret key.

2. A Simple Power Analysis (SPA) attack consists of recording a trace of a power consumption of a cryptographic processor with an oscilloscope. Then it is possible that the traces leak some information about the key, sometimes one can literally see the difference between 0 and 1, and read the key. This is, if there is no protection against SPA such as added (broad spectrum) electrical noise. Maybe one can use use circuitry such that 0 and 1 use the same amount of energy (not really enough) and have similar traces (much better). Some answers for which fractional points would be awarded, these do not really work well and very good SPA attacks will remain. For example it seems that SPA is also prevented by the security engineering in the Oyster card making that the card never answers to command unless the reader is authenticated first. In practice however SPA will

be done on the verification process, when checking if the reader cryptogram is valid... Similarly, we can observe that dummy operations or random instructions will NOT really thwart SPA, will just make it more complex or more precise, but usually they will result in very distinct traces that are easy to discard in an improved SPA attack focusing on some very special patterns. Human eye or neural networks can be used to learn to distinguish patterns.

3. A Differential Power Analysis (DPA) attack consists of guessing a few key bits, averaging many power consumption traces in a certain set/"basket", such that a certain value/byte or bit that is known/computed by the attacker is the same for all traces in one "basket". The main idea is that the averaged curve for each basket will be very similar if our guess on key bits is wrong, and dissimilar if the guess is correct. Thus (with possibly some false positives and some false negatives) we gain information about the secret key.

4. For example, if the CPU clock is random, or if the CPU sometimes stops and waits for a random time, or if we execute dummy instructions at random moments, it will be hard to re-synchronize different curves in time, to average them. Another answer: one student observed that we can also defend against DPA by doing probabilistic encryption: then each time the smart card runs the encryption, the plaintext is different. This can work as well. Keeping the crypto algorithm secret will also most likely thwart DPA attacks.

5. This is because RSA would be too slow (polynomial but slow). In hybrid encryption, a random 'session key' is used to encrypt a long message with a good probabilistic symmetric encryption scheme, for example a block cipher with a suitable mode, (Data Encapsulation) and this random 'session key' is sent encrypted with RSA (Key Encapsulation).

6. Electronic and Advanced Signatures (in The European Directive, December 13, 1999). Electronic Signature: Definition [EU]: data in electronic form which are attached to, or logically associated with, other electronic data and which serve as a method of authentication. Advanced Electronic Signature. Stronger. the two broad requirements are 2x link: link to the person that signs, and the link to the document. More precisely, an electronic signature will be considered to be an Advanced Electronic Signature if:

   (a) the signature is uniquely linked to a signatory and capable of identifying the signatory, and created by means the signatory can maintain under his sole control,

(b) the signature is linked to the data being signed such that any change of the data is detectable.

7. This MRZ that is read optically by the passport scanner, contains the passport number (9 chars typically), date of birth, expiration date, and 3 check digits (as CVV2 in bank cards). It is needed to enter an encrypted and authenticated communication session that allows to read the biometric files inside the passport.

8. All data are digitally signed, it is called Passive Authentication, PA. It is a static scheme, which is now mandatory in all passports. This signature key belongs to a Document Signer (DS) which is one of the qualified passport issuers/manufacturers. The same key will be used in many passports. This key is certified by the Country Signing CA (CSCA), and there is one root such root CA per country. There is no central authority, and all the public keys for each country must be installed in the terminal. A similar technique used in bank cards and is called SDA: it amounts roughly speaking to digitally signing with RSA (at least) all the basic card including credit card number, expiration date, etc. This signature is simply too long (e.g. 1000 bits) to be stored on the magnetic stripe, and it is stored in the chip.

9. The fingerprint and iris, or DG3 and DG4, are sensitive and require Extended Access Control (EAC).

10. The emails are encrypted and signatures are verified with public keys on PCs, but private keys are generated by a smart card, and the decryption and signatures take place on the card so that the private key never leaves the card. This type of solution is supported by PGP and Microsoft, and is used by many companies, such as Sun, Microsoft or within US government. Encryption and signatures are thus protected against malware running on a PC that would like to steal our private key. In addition, digitally signed email can help to fight spam, especially because the smart card is simply too slow to be able to sign too many emails.

3. Open Questions. In these questions the student has a substantial degree of freedom when answering. Students can use examples from their favorite industry; or focus on some particular technology; or expand on the question from a purely technical, theoretic or cryptographic perspective. Any mix of what could potentially be done, vs. current commercial technology is allowed.

1. Security Notion / Definition is a triple of 1.) Adversarial Goal, 2.) Resources of the Adversary, 3.) Access / Attack. Give two examples: one example from the IT industry or cryptography, and another one from the ’old economy’ (airport, car industry, shoplifting, old-fashioned banking etc).

   [5 marks]

2. Give **two** examples of techniques, methods or other things that may prevent a criminal from making a credit card, a bank note, an ID card, a building pass, or an electronic passport that looks like a real one (to another human).

   [5 marks]

3. Give **four** examples of techniques, methods or other things that may prevent a criminal from extracting the PIN from a SIM card, or a bank card (we assume that the PIN is stored inside).

   [5 marks]

4. Give **four** examples of techniques, methods or other things that may prevent a criminal from learning the PIN or the password, when using a 2-factor authentication, in access control, payment or in a PC logon system.

   [5 marks]

5. Give **four** examples of techniques, methods or other things that allow to or help to authenticate **individual** payment transactions. This means doing more than entity authentication (entity can be a user, his card/token, his PC etc), and more than static data authentication. You should specifically focus on the problem whether transaction can be modified, or replayed by a dishonest store or employee that wants simply to charge you more money than the agreed price, or repeat the transaction. You may consider all sorts of attacks: man-in-the-middle, social engineering, chip cloning, etc. The response can but does not have to refer to the current Chip and PIN technology. Alternatively, the question can be answered in a broader context of payment technology and/or electronic commerce with any combination of hardware devices, cryptographic protocols, data and entity authentication.

[5 marks]

[Total 25 marks]

Example Answers for 3.

1. For the car: 1.) can be to puncture a tyre, 2.) can be a nail, 3.) can be when you stop on the red light. Or for a laptop 1.) can be to learn the name of the employer of the user, 2). can be his own eyes, 3.) access can be a random commuters sitting next to each other on the train. For IND-CPA 1.) is to distinguish between encryption of two messages, 2.) will be a very powerful PC + good crypto expertise, 3.) will be adaptive access to two oracles for encryption and decryption.

2. Here are some possible answers...

   - general physical aspect of the card (like fonts, colors etc.).
   - A hologram,
   - invisible fluorescent ink that is visible with UV light,
   - owner's photograph or/and manual signature on the card,
   - microtext / microlines that are only readable under a microscope

3. Here are some possible answers...

   - physical tamper-resistance of the chip, like embedding it in resin,
   - the PIN will not be stored in cleartext, but rather encrypted or hashed
   - obfuscation of memory location in which it is stored,
   - a counter to count the number of wrong PIN attempts, disabling the card after 3 attempts, which prevents a dictionary attack on the PIN,

4. Here are some possible answers, on the example of a bank card:

   - put some barriers that make the PIN hard to see even for a person standing by, or put the ATM inside a closed room where people enter one at a time,
   - explaining shoulder surfing and other low-tech attacks on TV makes that less people will fall for them
   - in EMV, the PIN sent from the terminal to the card can be encrypted, prevents interception of PIN between the card and the terminal

- the PIN that is sent encrypted to your bank between the ATM and the bank.
- this encryption should be probabilistic, or done in a way that is different for each card. This will prevent an eavesdropper from knowing when the PIN is identical for two different cards,
- in one prototype of a future bank card there is a small numeric keyboard on the card,
- it also has a screen and a generator of one-time passwords on the card,

5. Some possible answers in the chip-and-pin perspective.

   - the screen on the terminal should display the amount agreed with the seller,
   - if there is a line indicating the amount of the tip on the credit card restaurant ticket requiring a manual signature, one needs to put 0 or cross it,
   - triple DES in the chip, authenticates each individual transaction with a MAC, signing the amount of money spent, the currency code, etc.
   - protection of this triple DES against side-channel attacks, is also needed
   - EMV PKI: in DDA cards individual transactions are signed with RSA,
   - the sufficient strength of SHA-1 against second pre-images. This prevents modifying the amount of the transaction,
   - the sufficient strength and sufficient key size in all the above crypto algorithms,
   - online authorization; can be refused if we replay the same transaction many times,
   - transaction counter and storing the transaction history inside the chip,

END OF PAPER