Försättsblad till skriftlig tentamen vid Linköpings Universitet

Datum för tentamen	9 januari 2014
Sal	
Tid	8–12
Kurskod	TSIT03
Provkod	TEN2
Kursnamn/benämning **Provnamn/benämning**	Kryptoteknik Tentamen
Institution	ISY
Antal frågor	7
Jour/Kursansvarig	Jonathan Fors/Jan-Åke Larsson
Telefon under skrivtiden	013-284017
Besöker salen ca kl	10
Kursadministratör/kontaktperson	Carina Lindström, 013-284423 carina.e.lindstrom@liu.se
Tillåtna hjälpmedel	Language dictionaries between English and another language (no personal notes, no scientific dictionaries)
Övrigt	
Rutat eller linjerat papper	Vilket som
Antal exemplar i påsen	

Written exam in TSIT03 Cryptology

8:00–12:00, 9 January 2014

Jan-Åke Larsson
Institutionen för Systemteknik,
Linköpings Universitet

Permitted equipment: General dictionaries between English and another language without personal notes. (Thus not specific scientific dictionaries with or without formulæ.)

Solutions: Solutions will be posted on the course home page after the exam.

Grading: Grade n requires at least $6n + 2$ points

Other information: Answers can be in English or Swedish

1. Historical ciphers
   (a) The Enigma cryptosystem is built from a keyboard, a plugboard, rotors, and a lampboard. What cryptographic operation does the plugboard do, and what does the (wiring in the) rotors do? (2p)
   (b) What is the components of the cryptographic key for the Enigma? (1p)
   (c) How was the key distributed to the operators during the second world war? (2p)
   (d) At the beginning of the war, which weakness was present in the key distribution method? (1p)
2. Block cipher modes
   (a) Electronic Codebook Mode should not be used. Why? (1p)
   (b) What mode of operation of a block cipher is recommended to give message integrity? Draw a diagram of this mode. (2p)
   (c) Describe CTR, CounTeR mode. What are the benefits of counter mode? What are the drawbacks? (3p)
3. Asymmetric ciphers
   (a) What are the parameters in ElGamal encryption, and how do you choose them? (3p)
   (b) How is encryption and decryption done in ElGamal? (2p)
   (c) ElGamal encryption uses a random number k (which should be in your answer above). If, by mistake, the sender reuses the k value, can an attacker notice this? Does this compromise the security? How? (2p)

4. Hash functions

   (a) Briefly describe the three different criteria that make cryptographic hash functions (increasingly) secure. (3p)

   (b) Describe and analyze a "birthday" attack. (2p)

5. Elliptic curve cryptography

   (a) What is an elliptic curve, briefly? (1p)

   (b) What mathematical problem is the basis of security in Elliptic curve cryptography? (1p)

   (c) Describe Elliptic curve Diffie-Hellman key exchange. (2p)

   (d) If you want 128 "bits of security", what key length do you need in ECC? How does this compare with RSA? (2p)

6. Electronic cash

   (a) The book gives six requirements for a system for electronic cash, list four of these. (2p)

   (b) Security of electronic cash is usually based on two specific basic cryptographic protocols, which? (2p)

7. Quantum key distribution

   (a) What are the five protocol steps that make up a full QKD system? (2p)

   (b) What is the most common encoding of the raw key on the quantum channel? Mention two important properties of this encoding. (2p)

   (c) How do Alice and Bob detect eavesdropping on the quantum channel? Why is this possible? (2p)

Solutions

1. Historical ciphers

   (a) The Enigma cryptosystem is built from a keyboard, a plugboard, rotors, and a lampboard. What cryptographic operation does the plugboard do, and what does the (wiring in the) rotors do? (2p)

   - The plugboard interchanges two symbols
   - The wiring in the rotors permutes several symbols

   (b) What is the components of the cryptographic key for the Enigma? (1p)

   - The plugboard connections, the order of the rotors (and which rotors are used) and the initial settings of the rotors

   (c) How was the key distributed to the operators during the second world war? (2p)

   - Each operator had a pre-distributed booklet with the "daily key". This was then used to transmit the message key (the starting rotor settings), which was different for each message.

   (d) At the beginning of the war, which weakness was present in the key distribution method? (1p)

   - The message key (three symbols) was repeated, to avoid transmission errors

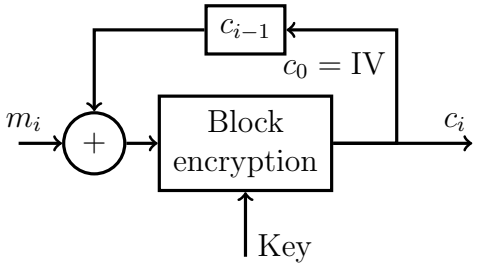
2. Block ciphers

   (a) Electronic Codebook Mode should not be used. Why? (1p)

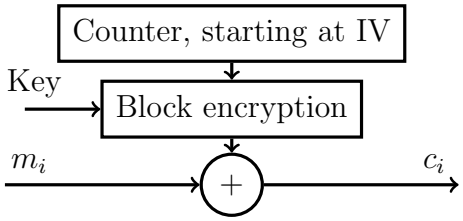
   - In ECB, repeated cleartext blocks imply repeated cryptotext blocks. This is information that an eavesdropper might find useful.

   (b) What mode of operation of a block cipher is recommended to give message integrity? Draw a diagram of this mode. (2p)

   - CBC, Cipher Block Chaining



   (a) Describe CTR, counter mode. What are the benefits of counter mode? What are the drawbacks? (3p)



- Benefits: very fast, can be implemented in parallel for several blocks. Drawbacks: Runs as a stream cipher, no message integrity check

3. Asymmetric ciphers

   (a) What are the parameters in ElGamal encryption, and how do you choose them? (3p)

   - Choose a large prime p, and a primitive root α mod p. Also, take a random integer a and calculate $\beta = \alpha^a$ mod p. The public key is the values of p, α, and β, while the secret key is the value a.

   (b) How is encryption and decryption done in ElGamal encryption? (2p)

   - Encryption uses a random integer k, and the ciphertext is the pair $(\alpha^k, beta^k m)$, both mod p
   - Decryption is done by calculating $(\alpha^k)^- a(\beta^k m) = (\alpha^{-ak})(\alpha^{ak} m) = m$ mod p

   (c) ElGamal encryption uses a random number k (which should be in your answer above). If, by mistake, the sender reuses the k value, can an attacker notice this? Does this compromise the security? How? (2p)

   - Yes, the first values in the cryptograms will be equal: $(\alpha^k, beta^k m_1)$, $(\alpha^k, beta^k m_2)$
   - The attacker can calculate m_1/m_2 by division of the two last values in the cryptograms. This can be used, if the message statistics is known, for example.

4. Hash functions

   (a) Briefly describe the three different criteria that make cryptographic hash functions (increasingly) secure. (3p)

   - (In all cases, it should be easy to calculate $h(x)$ from x)
   - One-way hash function: it is hard to find a preimage, to calculate x' from $h(x)$ so that $h(x') = h(x)$
   - Weakly collision-free hash function: it is hard to find a second preimage, to calculate x' from x so that $h(x') = h(x)$
   - Strongly collision-free hash function: it is hard to find x and x' ($x' \neq x$) such that $h(x') = h(x)$

   (b) Describe and analyze a "birthday" attack. (2p)

   - Fred (the Fraudster) knows that Alice will sign a contract. His goal is to get a signature from Alice on a different contract.
   - Fred takes the original contract and produces small variations in it. He can add spaces at the line ends, change the wording slightly, add nonprinting data, and so on. Thirty changes will give 2^{30} different documents.
   - He now does the same with the fraudulent contract, and attempts to find a match for the hash values of the two lists. The same signature will be valid for those two contracts

- If the hash values are shorter than 60 bits (two times 30), the probability of a match is very high.
- This must be taken into account in the security estimate

5. Elliptic curve cryptography

   (a) What is an elliptic curve, briefly? (1p)

   - An elliptic curve is the set of solutions to $y^2 = x^3 + bx + c$.

   (b) What mathematical problem is the basis of security in Elliptic curve cryptography? (1p)

   - The Elliptic Curve discrete logarithm: Given two points A and B on an elliptic curve, it is difficult (high complexity) to find a number k so that $B = kA = A + A + \ldots + A$.

   (c) Describe Elliptic curve Diffie-Hellman key exchange. (2p)

   - Choose an elliptic curve E mod a prime number p and a point α on the curve. Alice should randomly generate a secret integer a and make $a\alpha$ public (as a point on E). Likewise, Bob takes a secret random integer b and makes $b\alpha$ public. Both can now create $k = b(a\alpha) = a(b\alpha)$.

   (d) If you want 128 "bits of security", what key length do you need in ECC? How does this compare with RSA? (2p)

   - You need twice as many bits in the key, here 256 bits. This is much shorter than in RSA.

6. Electronic cash

   (a) The book gives six requirements for a system for electronic cash, list four of these. (2p)

   - Secure transfer in computer networks
   - Cannot be copied and reused
   - Anonymity
   - Offline transactions
   - Can be transferred to others
   - Can be subdivided

   (b) Security of electronic cash is usually based on two specific basic cryptographic protocols, which? (2p)

   - Security is usually based on "blind signatures" and "secret sharing"

7. Quantum key distribution

   (a) What are the five protocol steps that make up a full QKD system? (2p)

   - Raw key generation, Sifting, Reconciliation (or Error correction), Privacy amplification, Authentication

   (b) What is the most common encoding of the raw key on the quantum channel? Mention two important properties of this encoding. (2p)

- The most common encoding is into single photon polarization. Alice randomly alternates between horizontal/vertical polarization (for binary 0/1) or $+/-45^\circ$ polarization. It is important for the security that the encoding is into single photons, and that H/V or $+/-$ is chosen at random.

(c) How do Alice and Bob detect eavesdropping on the quantum channel? Why is this possible? (2p)

- They check the noise on the quantum channel during the reconciliation step. Too much noise: Eve has been eavesdropping. In this case, Alice and Bob abort the round and try again. BB84 can handle up to 11% quantum bit error rate.
- This is possible because of Heisenberg's uncertainty relation (when using random encoding onto single photons). If Eve chooses to measure in the wrong encoding, the information that Alice encoded will be destroyed. For example if Eve measures H/V polarization when Alice has encoded in +/- polarization, the bit that Alice encoded will be randomized. And this will introduce noise in the output data.