Försättsblad till skriftlig tentamen vid Linköpings Universitet

Datum för tentamen	30 augusti 2014
Sal	
Tid	8–12
Kurskod	TSIT03
Provkod	TEN2
Kursnamn/benämning **Provnamn/benämning**	Kryptoteknik Tentamen
Institution	ISY
Antal frågor	7
Jour/Kursansvarig	Jan-Åke Larsson
Telefon under skrivtiden	013-281468
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, 30 August 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 $6n + 3$ points

Other information: Answers can be in English or Swedish

1. Historical ciphers
   (a) Find the cleartext for the following cryptotext (hint: the language is English, 2p).

   ```
   ftqqj myuzq dpuex uwqee mfgdp mkqjm ye
   ```

   (b) What is the name of the cipher used? (1p)
   (c) How many different possible keys are there? (1p)
   (d) Why is it particularly easy to find the cleartext for the above cryptotext? (1p)
2. Feistel networks
   (a) Draw a Feistel network, and explain what part that performs "substitution", and what part performs "permutation". (2p)
   (b) How many rounds are needed in a Feistel network to make attacks nontrivial? (1p)
   (c) How many rounds does the Feistel network in DES have? (1p)
   (d) What kind of attack may still be relatively simple if the Feistel network has exactly the number of rounds in (b)? (1p)
   (e) What did IBM publish when this kind of attack had been (re-)discovered? (1p)
3. Asymmetric ciphers
   (a) How do you choose the RSA parameters p, q, n, e, and d? (Only the properties that make the construction work are needed, 2p)
   (b) In RSA, what is a suitable number of bits for the public key n to give reasonable security? Given your answer, how long would the security time horizon be? (2p)
   (c) Some choices of the parameters p and q makes the system easier to break. How should p and q be chosen, give two more important criteria? (2p)
   (d) Describe and analyze one attack that is possible if one of the criteria in (c) fails. (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. Message authentication, and digital signatures

   (a) What is the technical difference between a Message Authentication Code and a digital signature? (2p)

   (b) What are the effects of this, in terms of who can create a MAC, and who can create a signature? Who can verify a MAC, and who can verify a signature? (2p)

   (c) What is a "blind signature"? (1p)

   (d) Describe how a blind signature can be created using RSA. (2p)

6. Secret sharing

   The owner of company X normally handles the combination of the company safe himself, but in case he cannot come to work, any two out of the six employees should be able to open the safe, if they cooperate. The owner regularly changes the combination to the safe and then of course the employees should get new shares. Suppose that the combination is changed to 4237.

   (a) Give a suggestion for a possible value for each of the six shares and describe how two shares are used to retrieve the correct combination. (2p)

   (b) How does he need to change his system if instead any three out of the six employees should be able to open the safe? (2p)

7. Quantum key distribution

   (a) What does BB84 stand for? (1p)

   (b) Describe raw key generation, sifting, and eavesdropping-detection for BB84. Use the standard data encoding for the quantum channel. (4p)

   (c) Assume there are no transmission errors in the absence of an eavesdropper. What is the error rate if the eavesdropper is present? (1p)

Solutions

1. Historical ciphers

   (a) Find the cleartext for the following cryptotext (hint: the language is English, 2p).

   - "q" is the most common letter in the cryptotext, while "e" is the most common letter in English. Attempting to decrypt with Caesar using "q"−"e"="m" gives a valid text (which should be in your answer).

   (b) What is the name of the cipher used? (1p)

   - Caesar

   (c) How many different possible keys are there? (1p)

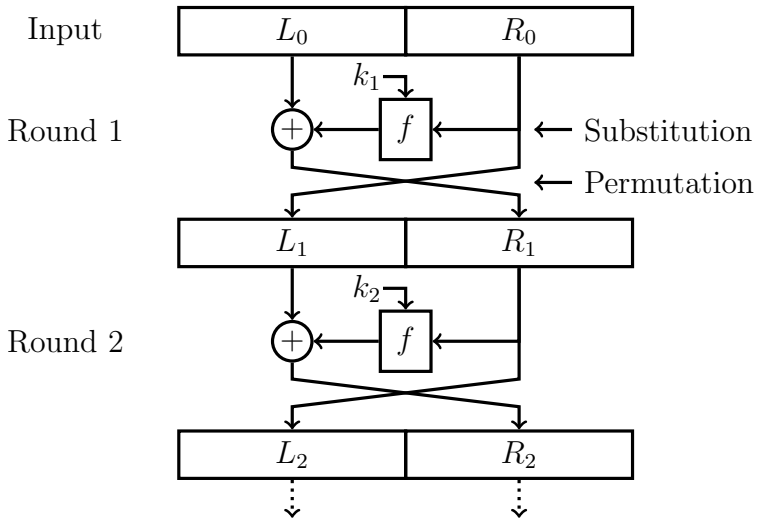
   - 26

   (d) Why is it particularly easy to find the cleartext for the above cryptotext? (1p)

   - Caesar is simple to break, and here you don't even need to try all the keys.

2. Feistel networks

   (a) Draw a Feistel network, and explain what part that performs "substitution", and what part performs "permutation". (2p)



   (b) How many rounds are needed in a Feistel network to make attacks nontrivial? (1p)

   - 4

   (c) How many rounds does the Feistel network in DES have? (1p)

   - 16

   (d) What kind of attack may still be relatively simple if the Feistel network has exactly the number of rounds in (b)? (1p)

   - Differential cryptanalysis

   (e) What did IBM publish when this kind of attack had been (re-)discovered? (1p)

- The design criteria for the S-boxes in DES that are part of the "f" function in the boxes above

3. Asymmetric ciphers

   (a) How do you choose the RSA parameters p, q, n, e, and d? (Only the properties that make the construction work are needed, 2p)

   - The parameters p and q are random very large primes, and $n = pq$. An important number here is $\phi(n) = (p-1)(q-1)$, and e is chosen so that $\gcd(e, (p-1)(q-1)) = 1$. The final parameter d is chosen so that $ed = 1 \mod (p-1)(q-1)$.

   (b) In RSA, what is a suitable number of bits for the public key n to give reasonable security? Given your answer, how long would the security time horizon be? (2p)

   - For long time security (30 years or so), 3kbit keys are recommended (the ECRYPT II 2010 report says 3248-bit keys).

   (c) Some choices of the parameters p and q makes the system easier to break. How should p and q be chosen, give two more important criteria? (2p)

   - To avoid being vulnerable to Fermat factorization, the primes p and q should be chosen to be of slightly different size.
   - To avoid being vulnerable to Pollard $p-1$-factorization, the primes p and q should be chosen so that $p-1$ and $q-1$ has at least one large factor.

   (d) Describe and analyze one attack that is possible if one of the criteria in (c) fails. (2p)

   - Fermat factorization can be used when $p \approx q$ and writes the number n as a difference of two squares to use the conjugate rule: $n = x^2 - y^2 = (x+y)(x-y)$. If p and q are close, then y will be a small number. The attack is done by calculating $n + 1^2$, $n + 2^2$, $n + 3^2$,..., until a square is reached. In that case, we have $n + y^2 = x^2$ and we can immediately factor. Making the difference large, for example using different size for p and q will prohibit this attack.

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. Message authentication, and digital signatures

   (a) What is the technical difference between a Message Authentication Code and a digital signature? (2p)

   - A digital signature is created in an asymmetric-key system while a MAC is created in a symmetric-key system

   (b) What are the effects of this, in terms of who can create a MAC, and who can create a signature? Who can verify a MAC, and who can verify a signature? (2p)

   - A digital signature can only be created by the one who knows the secret key, but can be verified by anyone that has the public key. A MAC can be created by anyone who can verify its correctness.

   (c) What is a "blind signature"? (1p)

   - Bob wants to prove that he has created a document at a certain time, but keep it secret, and Alice agrees to help him. She signs the document while the contents is hidden to her. Bob still gets a valid signature for his document.

   (d) Describe how a blind signature can be created using RSA. (2p)

   - Alice sets up standard RSA, keeping d for herself.
   - Bob chooses a random integer k, and gives Alice the message

   $$t = k^e m \bmod n$$

   - The number t is random to Alice, but she signs the message and gives the signature to Bob

   $$s = t^d = k^{ed} m^d = k m^d \bmod n$$

   - Bob can now divide by k and retrieve m^d, Alice's signature for m.

6. Secret sharing

   The owner of company X normally handles the combination of the company safe himself, but in case he cannot come to work, any two out of the six employees should be able to open the safe, if they cooperate. The owner regularly changes the combination to the safe and then of course the employees should get new shares. Suppose that the combination is changed to 4237.

   (a) Give a suggestion for a possible value for each of the six shares and describe how two shares are used to retrieve the correct combination. (2p)

(b) How does he need to change his system if instead any three out of the six employees should be able to open the safe? (2p)

- Create the line $y = kx + 4237$, with a random k. Then take six different random values for $x \neq 0$, find y for these and use these pairs as the shares. Any pair of employees can now reconstruct the line and find the value for $x = 0$.
- Create the curve $y = ax^2 + bx + 4237$, with random a and b. Then take six different random values for $x \neq 0$, find y for these and use these pairs as the shares. Any trio of employees can now reconstruct the line and find the value for $x = 0$.

7. Quantum key distribution

(a) What does BB84 stand for? (1p)

- Bennett-Brassard 1984

(b) Describe raw key generation, sifting, and eavsdropping-detection for BB84. Use the standard data encoding for the quantum channel. (4p)

- Alice uses random two bit-sequences, one for the raw key and the other for the data encoding. The data encoding on the quantum channel is either HV polarization or PM polarization ($\pm 45°$), depending on the data encoding bit. Bob also uses a random bitsequence for data decoding. After a run has finished, Alice and Bob compare encoding/decoding bits and throw away data where the encoding/decoding bits do not match. The remaining data should have low error rate, and if not, then somebody was eavesdropping.

(c) Assume there are no transmission errors in the absence of an eavesdropper. What is the error rate if the eavesdropper is present? (1p)

- 25%