Chapter 6

6.1 Methods of cryptanalysis

Cryptanalysis = the art and process of analyzing and decrypting ciphers, codes, and encrypted text without using the real key

Cryptanalyst = an expert in the field of cryptanalysis

Attack types

1. Ciphertext only -attack
2. Known/chosen plaintext -attack
3. Brute Force attack
4. Man in the Middle attack
5. Dictionary attack
6. Backdoors
7. Replay -attack
8. Side channel attack
9. Terminal attack

Ciphertext only attack (CEO)

Cryptanalyst has large amounts of encrypted data.

Classical ciphers (Enigma) can be broken with frequency analysis, if the cryptanalyst gets hold of adequately long encrypted messages

Known plaintext attack (KPA)

Cryptanalyst has in posession both plaintexts and their encrypted versions

In WW2 the Allies knew how Germans used to finish their messages with ”Heil...”

Brute force attack

The cryptanalyst has lots of computing power, he can search the whole key space for the key.

Method can be used if key space is much lower than 80 bits. (DES and GSM encryption A5)

Generally at mimimum 128 bit key is considered to have safety margin large enough against Brute Force attack.

Man in the Middle attack (MMA)

A third party E acts between communication of A and B pretending to be the other party to both directions. E can read and alter data.

CA -network which provides authentic public keys **is planned to prevent the MMA -attack.**

Dictionary attack

The hacker has a precalculated list of hash values of f.e 100 000 most common passwords.
He looks matches from servers password files.

Countermeasures against dictionary attack:
1) Using only ”strong passwords”
2) ”salting” the passwords with random characters before hashing or
3) hiding password hashes to a so called ”shadow file”.

Backdoors

Some algorithms may have a intentional backdoor, a security hole, which can be used to break the decryption.

It is reported that in 2006 NIST accepted Dual EC-DRBG as a standard random number generator for international use. Dual EC-DRBG was withdrawn shortly after Edward Snowden revealed in 2013 that it had a backdoor.

Replay attack

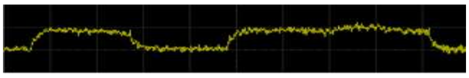
The hacker captures from the communication channel user login – data and reuses the data trying to log into the system.

Using time stamps and serial numbers prevents this attack

Thieves have used replay attack succesfully by recording the signals of car keys and reusing the signals. Today’s car locks are more sophisticated.

Side channel attack

Example: An equipment measures radiation of processor, when RSA private key is used to calculate power m ^{d} mod n. Analysis of the spectrum of radiation can give information about the private key d.



An attempt to decode RSA key bits using power analysis. The left peak represents the CPU power variations during the step of the algorithm without multiplication, the right (broader) peak — step with multiplication, allowing to read bits 0, 1.

Terminal takeover attack

Cryptoalgoritms are powerless, if the hacker has taken over the terminal of the user. Takeover is a significant cyber thread for businesses and individuals.

NSA's attack forms *(NSA = National Security Agency of USA)*

Public documents contain some information about NSA:s attack types. Basic forms are following

* Terminal takeover attacks
* Tampering messages sent by email servers
* Cooperation with service providers (Google, Facebook, RSA-lab,CA:s)
* Mathematical methods[1)]

1) It is generally assumed that mathematical methods are used for attempts to break 1024 –bit RSA public keys. Some experts think that this may already have succeeded.

6.2 Applications of cryptoalgorithms in other contexts than data encryption

6.2.1 Password Tokens

The device produces fixed length one-time passwords (OTP) for login.

TOTP (Time based One Time Password): The device creates a new password f.e every half minute. Device and service should have syncronized clocks.

COTP (Counter based One Time Password): The device creates a new password every time when the button is pressed. Counter value acts as an input for the next password.

6.2.2 HMAC - generated one-time passwords

Generation of OTP is usually based on HMAC function which creates a fixed length hash from the **SIM key K** and **counter value C**. Instead of counter can be also **time T**. The formula of HMAC is following.

$$\boxed{\text{HMAC}(K, C) = \text{sha}(K \oplus \text{opad} || \text{sha}(K \oplus \text{ipad} || C)}$$

HMAC has 60- bits. **Truncate – function** reduces HMAC value to a 6 digit password.

The server you want to log in to has a precalculated list of passwords corresponding f.e. 128 counter values. The user is accepted to service, if the password send by the user is found in the list

Security of HMAC

HMAC is secure. It is impossible the calculate SIM- key or counter value from the password.

From one password it is impossible to calculate the next password.

HMAC values fulfill all three propeties of pseudorandomness.

6.2.3 Remote Key Entry (RKE)

1. IN FIRST GENERATION RKE the signal from the key is always the same.
Skilled criminals could record the signal and as soon as the owner was not present the thieves replayed the signal to open the doors.

2. IN SECOND GENERATION RKE the key had Counter based One Time Password (=COTP) generator. The lock of the car precalculated a list of 256 one-time passwords. If a signal received from the key was found on the list, the doors opened or were locked.

If the button of the key was pressed more than 256 times outside the range of the signal, the list ran out of keys and the owner had to call the service of car manufacturer to open the doors.

3. In third generation RKE the car keys create **Time-Base one-time passwords** (=TOTP)**:** the key and the lock generate a new password f.e every half minute.
Use of TOTP prevents a vulnerability described below

Vulnerability of COTP.

Samy Kamkar showed in Defcon 2015 conference an equipment which can be used for replay attack against 2nd generation RKE.

Equipment used 3 radio devices.Two of them sends strong disturbance signals which prevent the signal from the key reach the lock. Third radio records and saves the signal.
When the owner pressed the button to shut the doors, lock does not react. Then the owner presses button again, the lock does not react to the second signal. The device of the thieves has recorded both signals. It sends quickly the first signal to the lock, which reacts and doors are closed. As a result the thieves have one unused recorder signal in the device. They can replay it to steel the car.

6.2.4 Secret sharing system

Secret sharing is an secure method of storing classified and important information. Examples: 1) safe deposits of important encryption keys 2) storage of missile launch codes 3) using anonymous bank accounts (Swiss banks)

Principle: Key for access to classified information is shared to parts (subkeys) in such that n individuals have parts of the key. The key can be reconstructed if a minimum number k (which is < n) of these individuals use their subkeys

Examples.
In a superpowers defence organization seven persons have subkeys to the launch code deposit. Deposit can be opened if any three of them use their subkeys.

Withdrawals can be made from an anonymous number account in a Swiss bank, when at least 3 persons (some of them may be bank clerks). The person making the withdrawal does not have to reveal his identity.

"Shamir's secret sharing scheme"

A parabola y = f(x) = a x^2 + b x + c is uniquely determined if three points on the parabola are known.

Assume seven persons are given one point (x,y) of a parabola.

If any three of them give their points, the system can solve a, b and c.

The shared key can be a value of f(x) = a x^2 + b x + c at a certain point , for example f(10).

Shamir's scheme uses discrete parabola y = a x^2 + b x + c (mod q). It consists of integer pairs (x,y), which satisfy y = a x^2 + b x + c (mod q) where a,b, a and modulus q are integers.

Example of Shamir's scheme

Modulus q = 113. Shared key K is f(10) of parabola f(x) = a x^2 + bx + c (mod q)

Seven persons are given following subkeys (one for each):

{7,91} {49,41} {110,85} {51,49} {18,74} {58,87} {72,59}

Users 1,3 and 7 login to the system using subkeys {7,91}, {110,85}, {72,59}.

Now we can calculate parameters a,b and c and calculate the master key K = f(10)

Calculation of a,b and c needs solving a linear system of three variables in Zq. It is possible manually with some effort. Here we use Mathematica software:

```
Reduce[a * 7^2 + b * 7 + c == 91 ∧
   a * 110^2 + b * 110 + c == 85 ∧
   a * 72^2 + b * 72 + c == 59,  {a, b, c},
 Modulus → 113]

a == 45 && b == 24 && c == 91
```

Result: **a = 45, b = 24 and c = 91**.

The master key K is f(10) = (45*10^2 + 24*10 + 91) mod 113 = **85**

6.2.5 Net voting

In Net Voting the voter proves his identity with electronic ID card or mobile certificate.

Estonia is pioneer of net voting. Net voting has been widely used only in Estonia, where the system has been used for many years. In the last parlamentary election 51% of the voters voted in the Internet.

A group of data security experts (among others Finnish Harri Hursti) has critizised the safety of net voting in their article: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

"As we have observed, the procedures Estonia has in place to guard against attack and ensure transparency offer insufficient protection. Based on our tests, we conclude that a state-level attacker, sophisticated criminal, or dishonest insider could defeat both the technological and procedural controls in order to manipulate election outcomes"

Nederlands moved from net voting back to paper ballots because of security concerns.

6.3 Future prospects

Algorithms are not changed unless there is a compelling need for change.
("Old, tested algorithms are better than a dozen of new")

When quantum computers develop, major changes must be done:

Survivals in post-quantum era:
AES258 and AES512 survive as standard block ciphers

Useless in post-quantum era:
Key Exchange protocols RSA, DH, ECDHE become useless.
Some digital signatures , f.e sha256RSA cannot be used

There exist already proposed replacements for RSA, e.t.c
They are ***Lattice Based*** and ***Multivariate algorithms***

At the moment there is an on-going international competition of finding new post quantum standards - similar than the competition in 1997 in which AES was chosen to block cipher standard.