Collection of questions (June 2020)

In the following collection are gathered some questions from the (available) past exams, and teaching material provided by Prof. Zseby (in bold), integrated with some questions added from the slides' content (in regular thickness). (https://vowi.fsinf.at/images/6/69/TU_Wien-Network_Security_VU_%28Zseby%29_-_Fragensammlung.pdf)

No warranty for correct answers!! Please double check with the slides!

01. Attack types

1. **What is the difference between viruses and worms?**

- **Virus:** "A self-replicating (and usually hidden) section of computer software (usually malicious logic) that propagates by infection -- i.e., inserting a copy of itself into and becoming a part of -- another program. A virus cannot run by itself; it requires that its host program be run to make the virus active." [RFC4949]
- **Worm:** "A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume system resources destructively." [RFC4949]

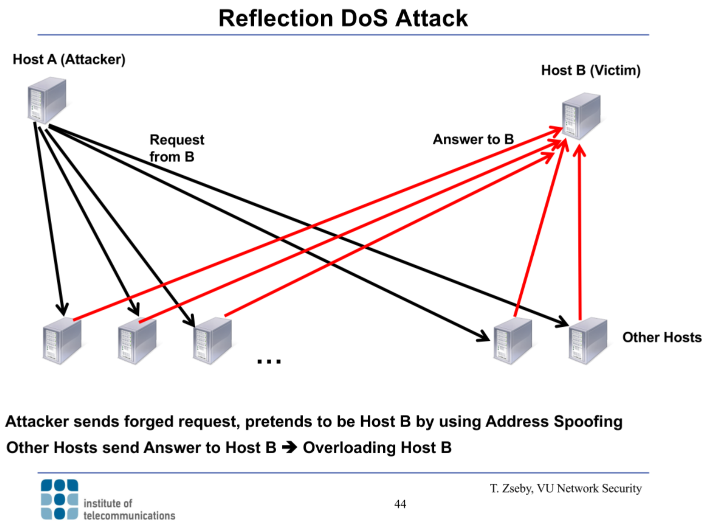
2. **Explain SYN floods**

- Attacker sends many SYN requests to the server, server sends SYN-ACK back and waits for ACK. Attacker never sends ACK. Server cannot answer any new SYN requests.
- This is only an attack on listening applications on a host, not on the host itself nor the network.
- Prevent establishment of new incoming connections to a specific port
- No impact on outgoing connection requests or previously established connections

3. **What is a horizontal scan?** A vertical scan?

- **Horizontal Scan** (Host Scan):
    - Search if a specific port is open on multiple hosts
    - Packages to
        - A single destination port
        - On multiple destination IP addresses
- **Vertical Scan** (Port Scan):
    - Search if any port is open on specific hosts
    - Packets to
        - Multiple destination ports
        - On a single destination IP address

4. **Explain the DDoS reflection attack.**
   The attacker sends forged requests to many hosts with the victims source address (Address Spoofing). All the hosts answer to the victim and therefore the victim gets overloaded.



Reflection DoS Attack

Attacker sends forged request, pretends to be Host B by using Address Spoofing
Other Hosts send Answer to Host B ➔ Overloading Host B

institute of telecommunications 44 T. Zseby, VU Network Security

5. What is meant by backscatter?
   Reply to spoofed addresses (see TCP-SYN Flood Attack)
6. What are the phases of worm propagation?
   1. Target finding
      i. E.g. scanning, target lists
   2. Transferring
      i. Sending a copy of the worm to the target
   3. Activation
      i. Start malicious activities
      ii. Triggered by date or condition
   4. Infection
      i. Result of malicious activity
7. **What is a monomorphic worm?** Polymorphic? Metamorphic?

- Monomorphic:
  - Payload does not change
  - May be fragmented in different ways
  - Signature-based detection
- Polymorphic
  - Payload changes (e.g., alternating encryption)
  - Behaviour (and algorithm) remain the same
- Metamorphic
  - Payload changes

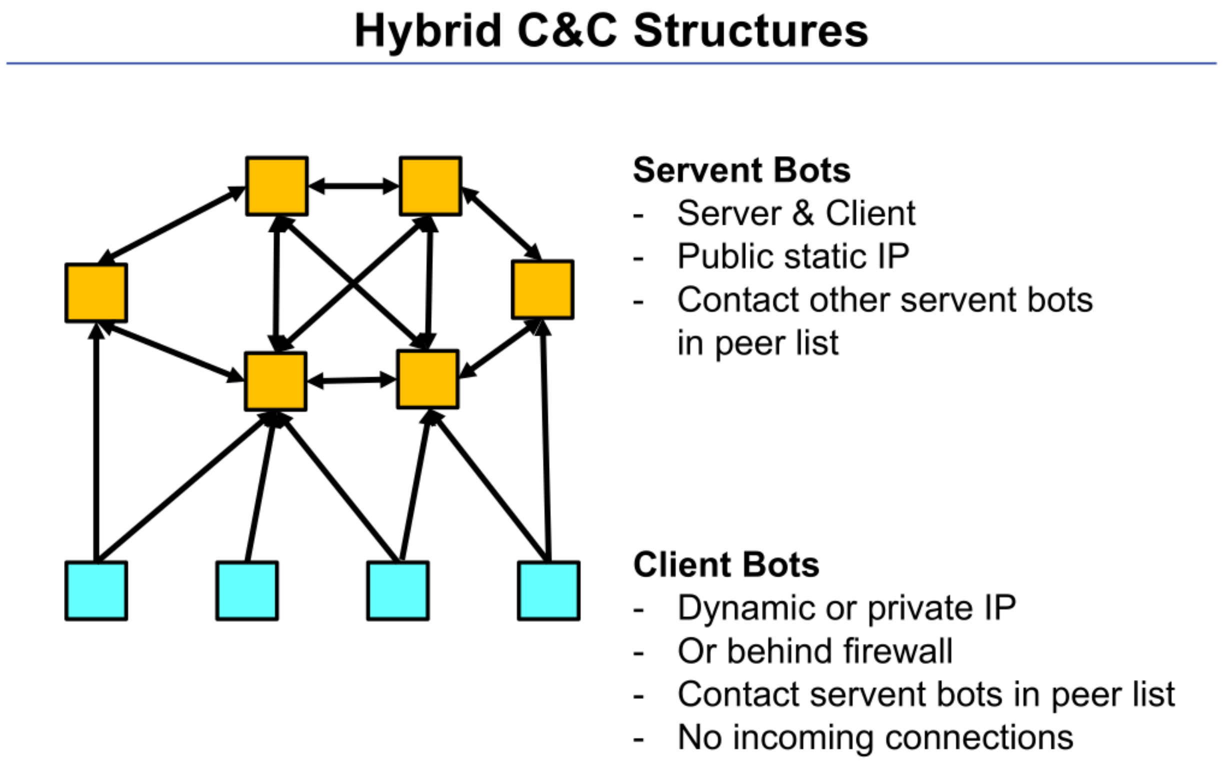
    - Behaviour changes

8. **Name 2 different topologies for a Botnet Command & Control structure. What are their advantages and disadvantages?**

- Centralized
    - Pro: Low latency
    - Con: Easier to detect
    - Con: Single point of failure (detection, takeover)
- Peer2Peer:
    - Pro: Robust
    - Con: Latencies, Loss
    - Con: Scalability
    - Con: complexity (manageability)

9. In hybrid Command & Control structures, what are servant and client bots?

- Servant Bots:
    - Server & Client
    - Public static IP
    - Contact other servant bots in peer list
- Client Bots:
    - Dynamic or private IP
    - Or behind firewall
    - Contact servant bots in peer list
    - No incoming connections



Hybrid C&C Structures

Servent Bots
- Server & Client
- Public static IP
- Contact other servent bots in peer list

Client Bots
- Dynamic or private IP
- Or behind firewall
- Contact servent bots in peer list
- No incoming connections

10. List and explain the different evasion methods that are used to conceal the C&C.

- Single Flux
- Double Flux
- Domain Flux
- Rogue DNS Servers
  - Own DNS service for bots
  - Hosted in countries with less strict laws
- Anonymization Services
  - Conceal sender
  - Run C&C as concealed service in Tor Network
- But suspicious Tor activities → detection possible
  - Many bots joining Tor
  - Bots downloading and running Tor software
  - → Bots detectable by traffic patterns

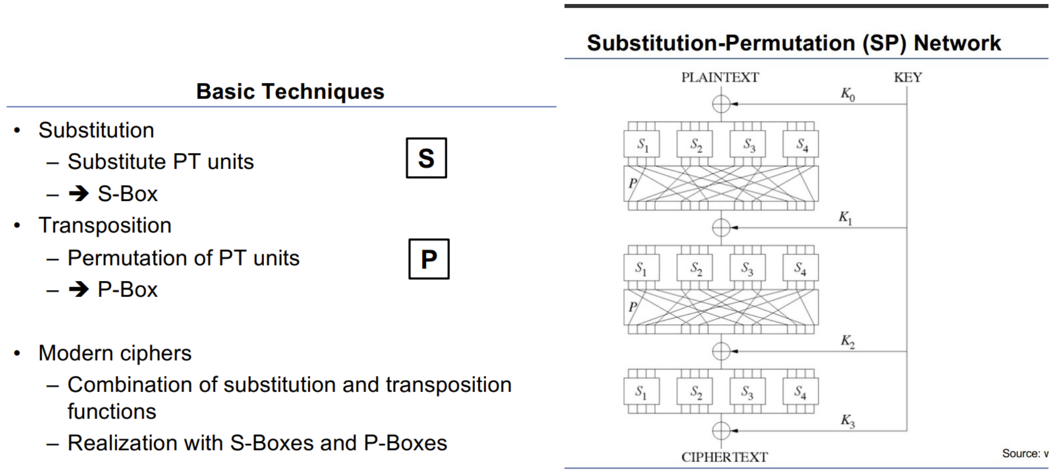
11. What are the most common obfuscation methods for botnet control traffic?

- Encryption
  - Evading content-based analysis

- Tunneling
  - HTTP → allowed by most middle boxes
  - IPv6 → less supported by IDS, firewalls
- Traffic Manipulation
  - Low volume traffic
- New communication methods
  - Social networks
  - Steganography

02. Ciphers

12. What are the basic building blocks of cryptography? And In modern ciphers?

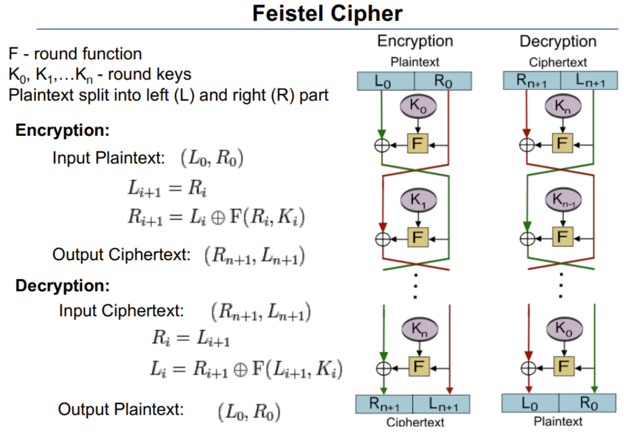


Basic Techniques

- Substitution
  - Substitute PT units
  - ➔ S-Box
- Transposition
  - Permutation of PT units
  - ➔ P-Box
- Modern ciphers
  - Combination of substitution and transposition functions
  - Realization with S-Boxes and P-Boxes

Substitution-Permutation (SP) Network

Source: v



Feistel Cipher

F - round function

K_0, K_1,…K_n - round keys

Plaintext split into left (L) and right (R) part

Encryption:

Input Plaintext: (L_0, R_0)

$$L_{i+1} = R_i$$

$$R_{i+1} = L_i \oplus \mathrm{F}(R_i, K_i)$$

Output Ciphertext: (R_{n+1}, L_{n+1})

Decryption:

Input Ciphertext: (R_{n+1}, L_{n+1})

$$R_i = L_{i+1}$$

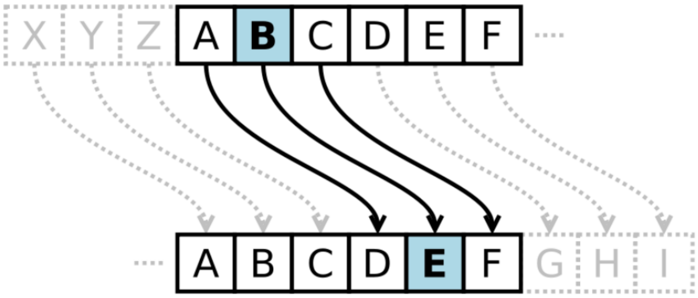
$$L_i = R_{i+1} \oplus \mathrm{F}(L_{i+1}, K_i)$$

Output Plaintext: (L_0, R_0)

13. Decrypt a message with the Caesar cipher, k=3

Simple Substitution Cipher (Caesar cipher)

- Shift letter by a fixed offset k



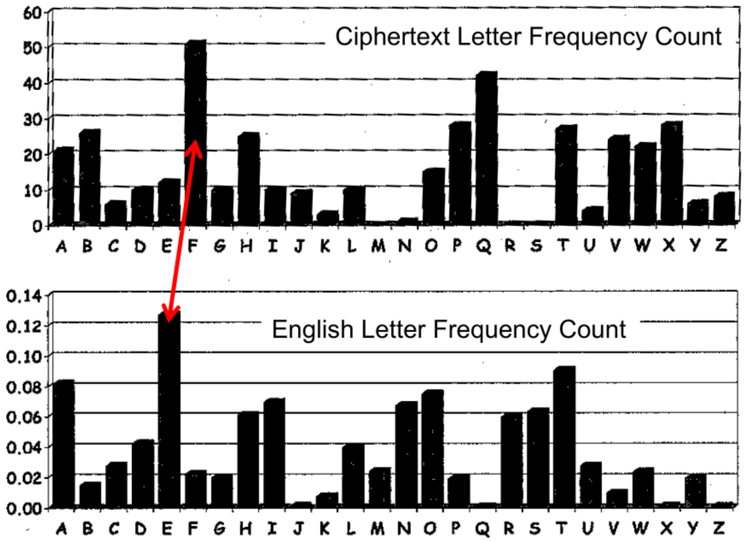
Source: wikipedia

- Example: k=3

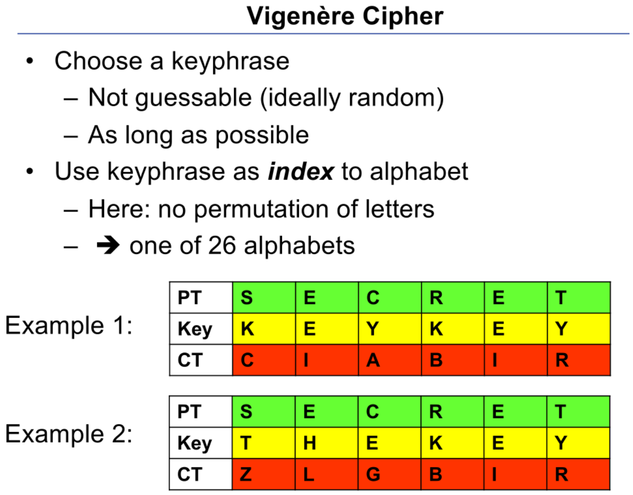
PT	**S**	**E**	**C**	**R**	**E**	**T**
CT	**V**	**H**	**F**	**U**	**H**	**W**

14. What is Letter Frequencies analysis?

Letter Frequencies



15. How does Vignère cipher work? How can it be broken? Calculate the ciphertext given a message and a key.



Vigenère Cipher

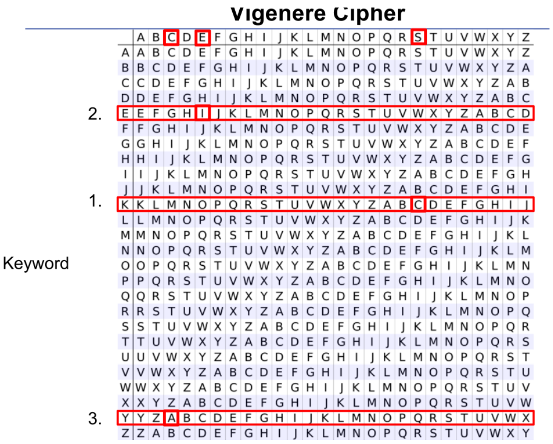
- Choose a keyphrase
  - Not guessable (ideally random)
  - As long as possible
- Use keyphrase as ***index*** to alphabet
  - Here: no permutation of letters
  - ➔ one of 26 alphabets

Example 1:

PT	S	E	C	R	E	T
Key	K	E	Y	K	E	Y
CT	C	I	A	B	I	R

Example 2:

PT	S	E	C	R	E	T
Key	T	H	E	K	E	Y
CT	Z	L	G	B	I	R



Vigenere Cipher

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
2.	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
1.	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Keyword	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
3.	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

How can it be broken?

1. When the key is too short, it is possible to find a repeated pattern
2. it is then possible to count the max key length (start points from repeated pattern).
3. Check possible key length
4. Split text into alphabets
5. Do frequency analysis

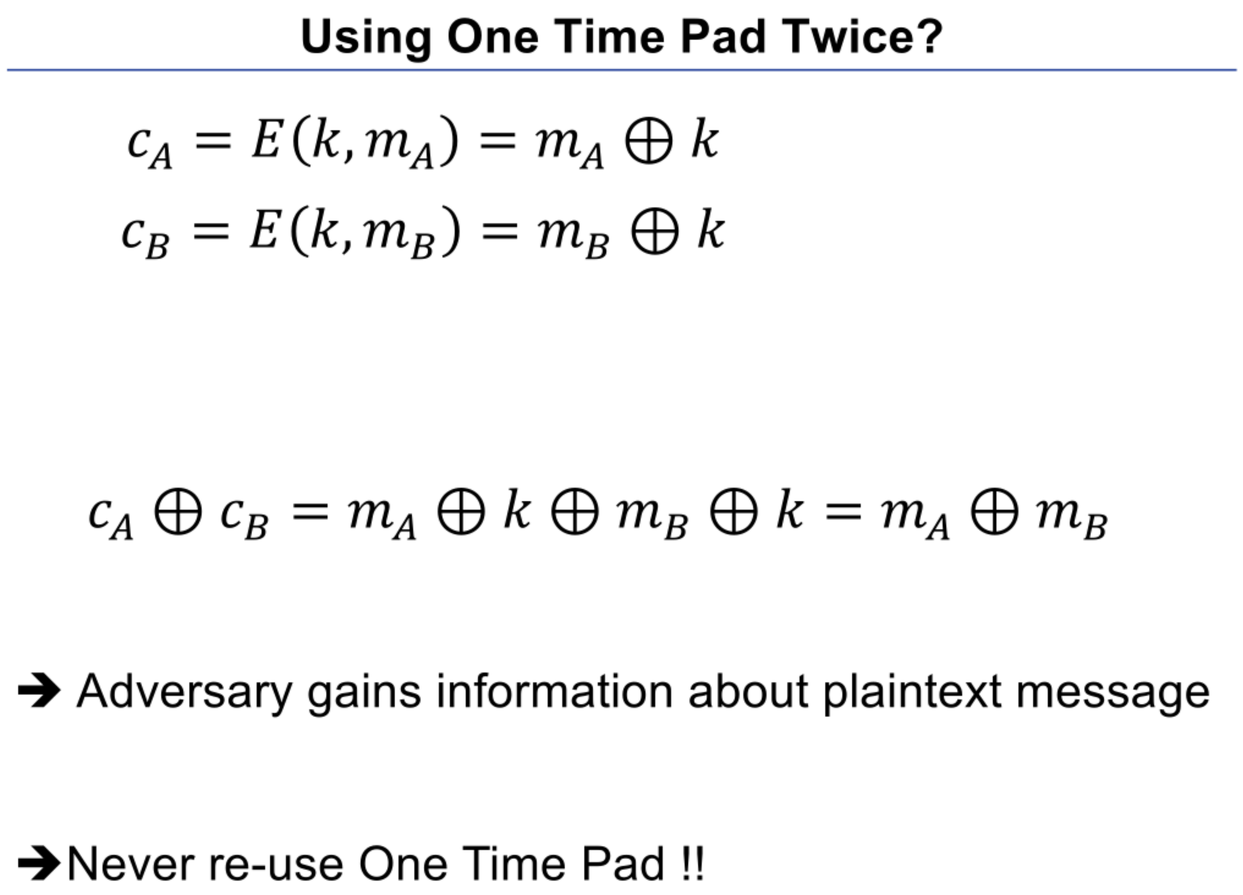
16. **How does a One-Time-Pad work? Calculate the ciphertext for a message and a key.**

Key has the same length as the message (in bit). Crypto Message is Message XOR Key.

17. **What distinguishes a good and a bad key for OTP? Name 4 properties for a good key.**

- Key has same length as message
- Key is chosen randomly
- Key remains a secret
- Key is only used once

18. **Why is it a bad idea to use a OTP key twice?**



Using One Time Pad Twice?

$$c_A = E(k, m_A) = m_A \oplus k$$

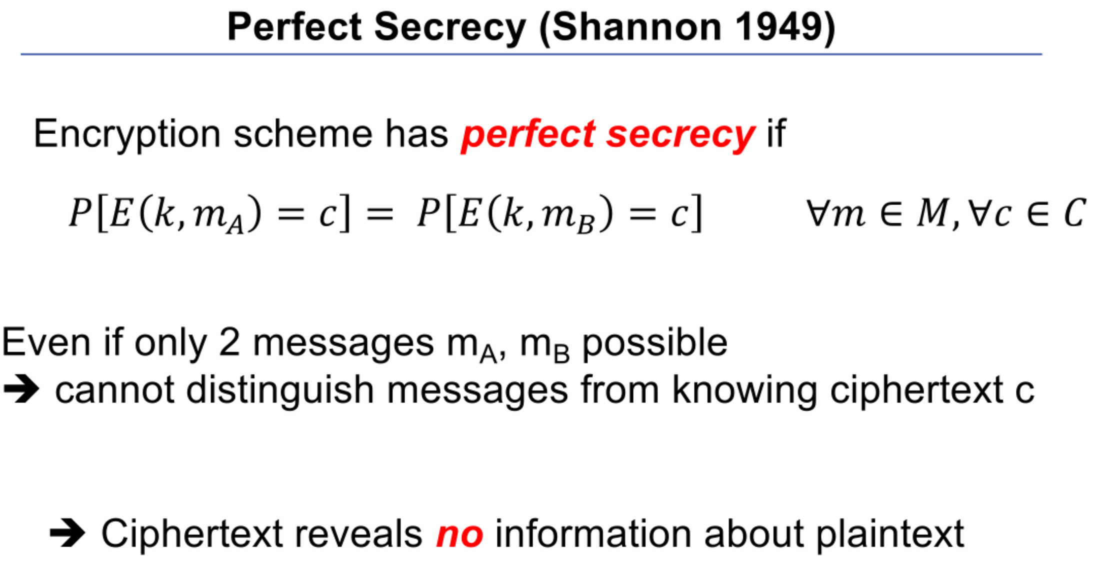
$$c_B = E(k, m_B) = m_B \oplus k$$

$$c_A \oplus c_B = m_A \oplus k \oplus m_B \oplus k = m_A \oplus m_B$$

➔ Adversary gains information about plaintext message

➔Never re-use One Time Pad !!

19. What is meant with perfect security (or perfect secrecy)? And with computational security?



Perfect Secrecy (Shannon 1949)

Encryption scheme has ***perfect secrecy*** if

$$P[E(k, m_A) = c] = P[E(k, m_B) = c] \qquad \forall m \in M, \forall c \in C$$

Even if only 2 messages m_A, m_B possible
➔ cannot distinguish messages from knowing ciphertext c

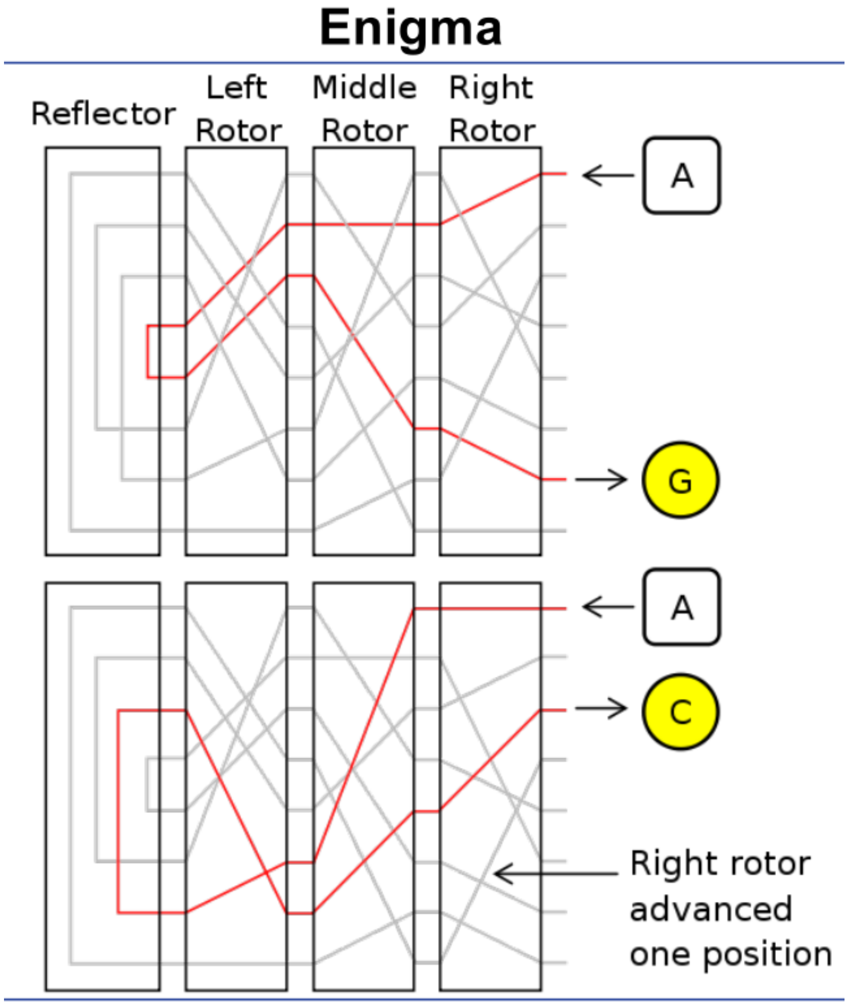
➔ Ciphertext reveals ***no*** information about plaintext

20. What is the main Kerchoff's principle?

Cipher system must be:

- Practically (if not mathematically) indecipherable
- Not required to be secret and able to fall into the hands of the enemy without inconvenience.
- Key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents.
- Applicable to telegraphic correspondence
- Portable, and its usage and function must not require the concourse of several people
- Easy to use (requiring neither mental strain nor the knowledge of a long series of rules to observe)

21. Explain, with a simple drawing, how do rotor machines for encryption work.



22. What is the difference between a substitution cipher and a transposition cipher?

    Substitution Cipher:

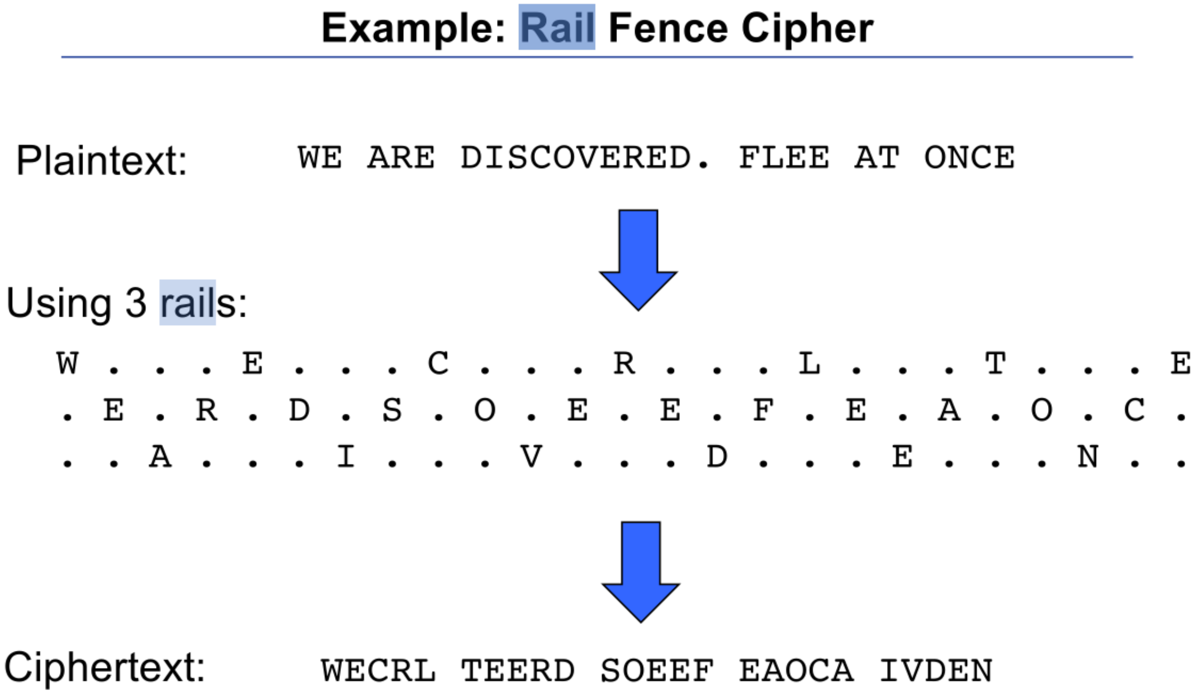
    - Every incoming letter has a (fix) substitute

  - Also called S-Box

Transposition Cipher:

  - Ciphertext is permutation of units (letters) in plaintext
  - Key provides rules to change position of units
  - P-Box

23. Encrypt a message using a Rail-Fence cipher with 3 rails.



Example: Rail Fence Cipher

Plaintext: WE ARE DISCOVERED. FLEE AT ONCE

Using 3 rails:

```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

Ciphertext: WECRL TEERD SOEEF EAOCA IVDEN

24. **Can you use only Letter Frequencies analysis on a transposition cipher to get info about plaintext?**

    No, letter frequencies do not offer more information (in a tp cipher the letters are the same as in the plain text)

25. **Explain the ciphertext-only, known-plaintext, chosen plaintext, and chosen ciphertext attacks.**

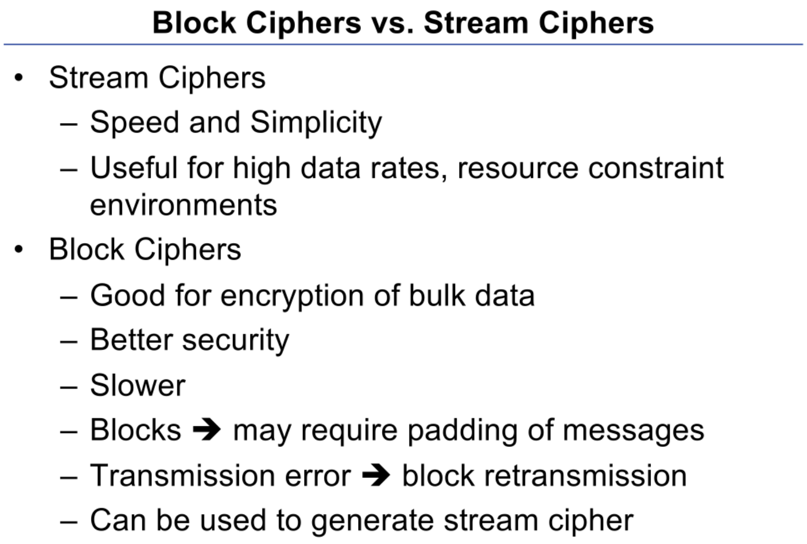
- **Ciphertext-only attack:**
  - Adversary has access to set of ciphertexts
  - E.g. from eavesdropping messages exchanged between A and B
- **Known-plaintext attack:**
  - Adversary has access to a set of ciphertexts to which he knows the corresponding plaintext
- **Chosen Plaintext attack:**
  - Adversary can obtain ciphertexts for an arbitrary set of plaintexts that he selected
- **Chosen Ciphertext attack:**

    - Adversary can obtain plaintexts for an arbitrary set of ciphertexts that he selected

26. What is a related key attack?
    - Adversary can obtain ciphertexts encrypted by two different keys.
    - Key remain unknown, but relationship between keys is known (e.g. differ in one bit)

27. **Explain what is the difference between stream and block ciphers.**

- **Block cipher:**
    - Algorithm operates on message blocks of fixed length
    - Usually a product cipher with multiple iterations of S-Box and P-Box operations
    - Example: 3DES, AES,...
- **Steam cipher:**
    - Generate a keystream
    - One key bit for each plaintext bit
    - Combine plaintext bits with key bits
    - Faster
    - Example: RC4



Block Ciphers vs. Stream Ciphers

- Stream Ciphers
    - Speed and Simplicity
    - Useful for high data rates, resource constraint environments
- Block Ciphers
    - Good for encryption of bulk data
    - Better security
    - Slower
    - Blocks ➔ may require padding of messages
    - Transmission error ➔ block retransmission
    - Can be used to generate stream cipher

28. **Calculate the advantage given P(A(R) = 1) = 0.9 and P(A(G(s)) = 1) = 0.2. Can G be considered a good PRG?**

Advantage Examples

$$Adv\big(A, G(s)\big) = \big|P\big(A\big(G(s)\big) = 1\big) - P\big(A(R) = 1\big)\,\big|$$

$P\big(A(R) = 1\big) = 0.9$ ➔ Test suitable to discover randomness

$P\big(A\big(G(s)\big) = 1\big) = 0.1$ ➔ But does not consider G(s) as random

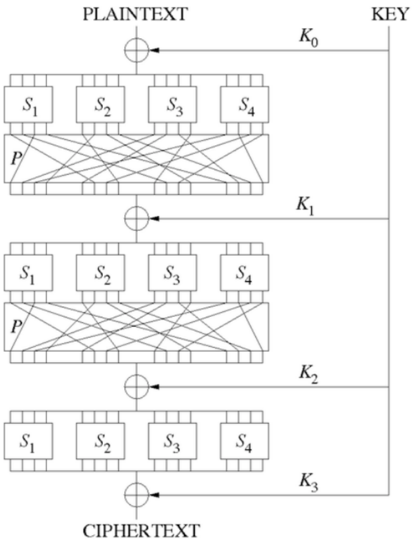
$$Adv\big(A, G(s)\big) = |0.1 - 0.9\,| = 0.8$$

➔ Weak PRG

03 Symmetric cryptography

29. Draw the scheme of a SP (substitution-permutation) network

AES is a Substitution-Permutation Network



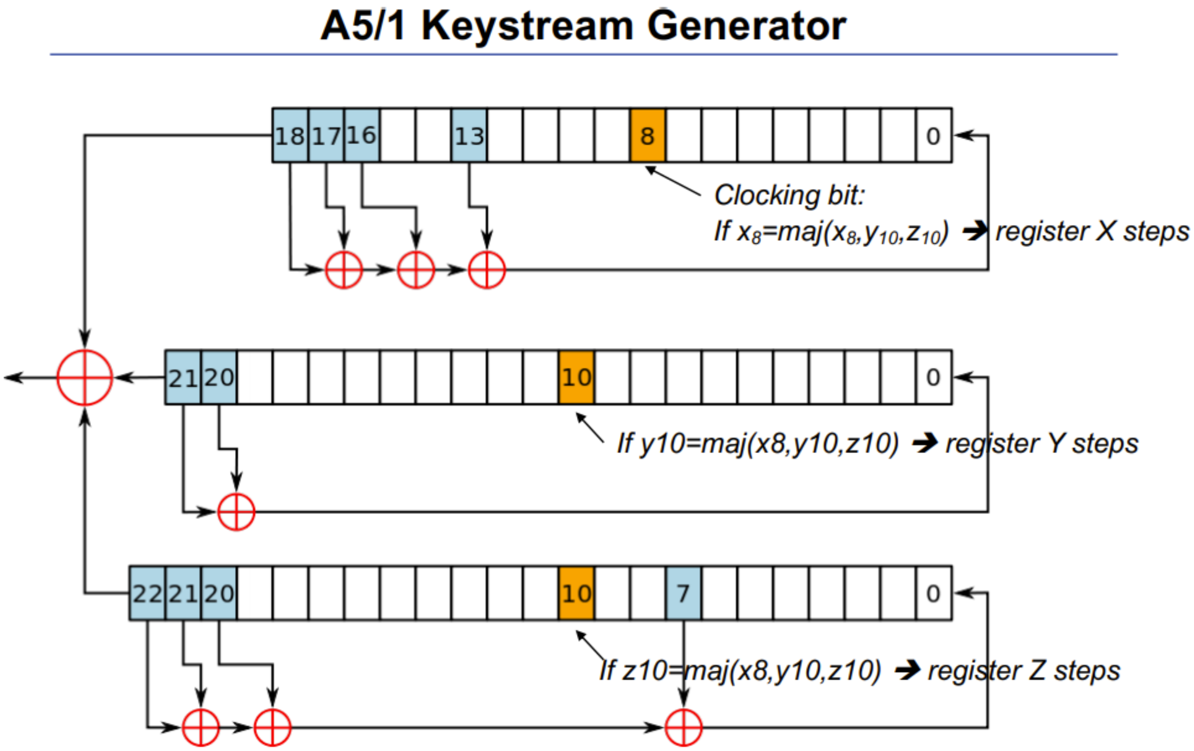
Substitution Layer

Permutation Layer

Key Addition Layer

Source: wikipedia

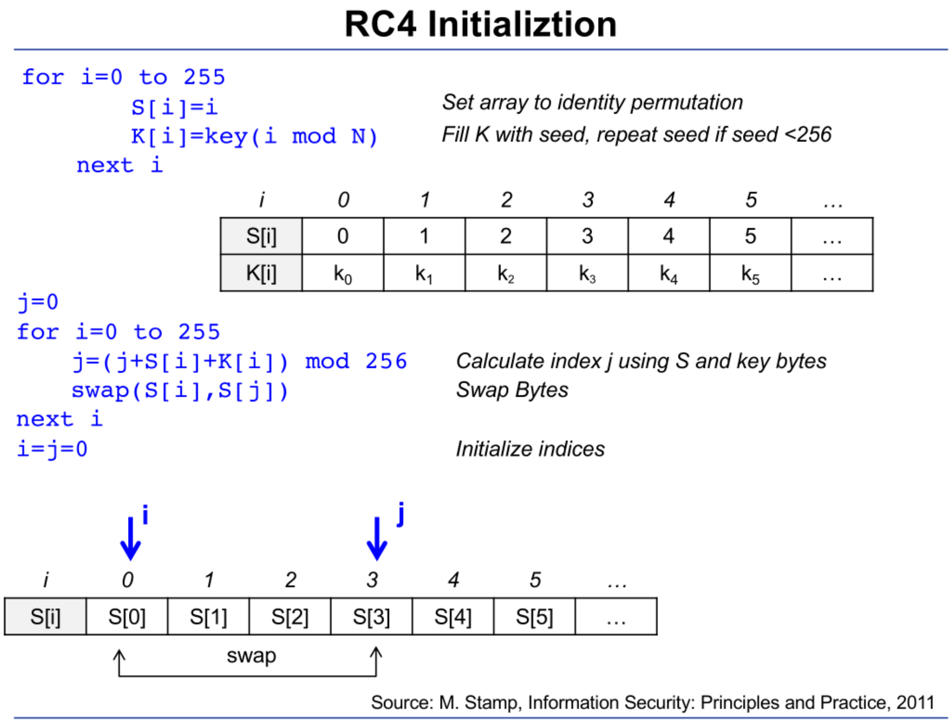
30. A5/1: How is the encryption built?


A5/1 Keystream Generator

18
17
16
13
8
0
Clocking bit:
If x_8=maj(x_8,y_{10},z_{10}) ➔ register X steps
21
20
10
0
If y10=maj(x8,y10,z10) ➔ register Y steps
22
21
20
10
7
0
If z10=maj(x8,y10,z10) ➔ register Z steps

64 Bits (19 + 22 + 23) and each register has some bits that get XORed and pushed into the beginning of the register. The last bit of each register gets XORed with the other last ones and is used for the key.

31. RC4: How is the algorithm initialized?
    - There are two byte arrays, S and K
    - S is set from 0 to 255
    - RC4 Initialization (where seed is the master key of length 40 - 128 bits):



RC4 Initializtion

```
for i=0 to 255
        S[i]=i                          Set array to identity permutation
        K[i]=key(i mod N)               Fill K with seed, repeat seed if seed <256
    next i
```

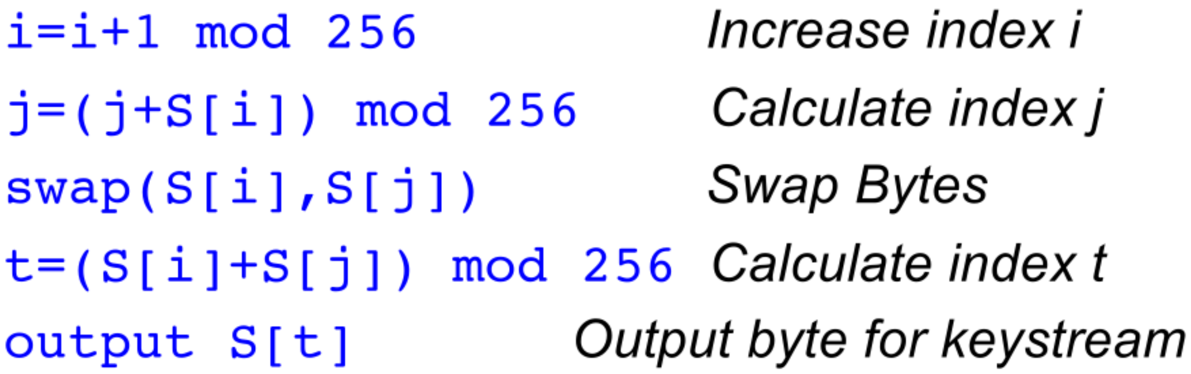
i	*0*	*1*	*2*	*3*	*4*	*5*	…
S[i]	0	1	2	3	4	5	…
K[i]	k_0	k_1	k_2	k_3	k_4	k_5	…

```
j=0
for i=0 to 255
    j=(j+S[i]+K[i]) mod 256          Calculate index j using S and key bytes
    swap(S[i],S[j])                  Swap Bytes
next i
i=j=0                                Initialize indices
```

i	*0*	*1*	*2*	*3*	*4*	*5*	…
S[i]	S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	…

Source: M. Stamp, Information Security: Principles and Practice, 2011

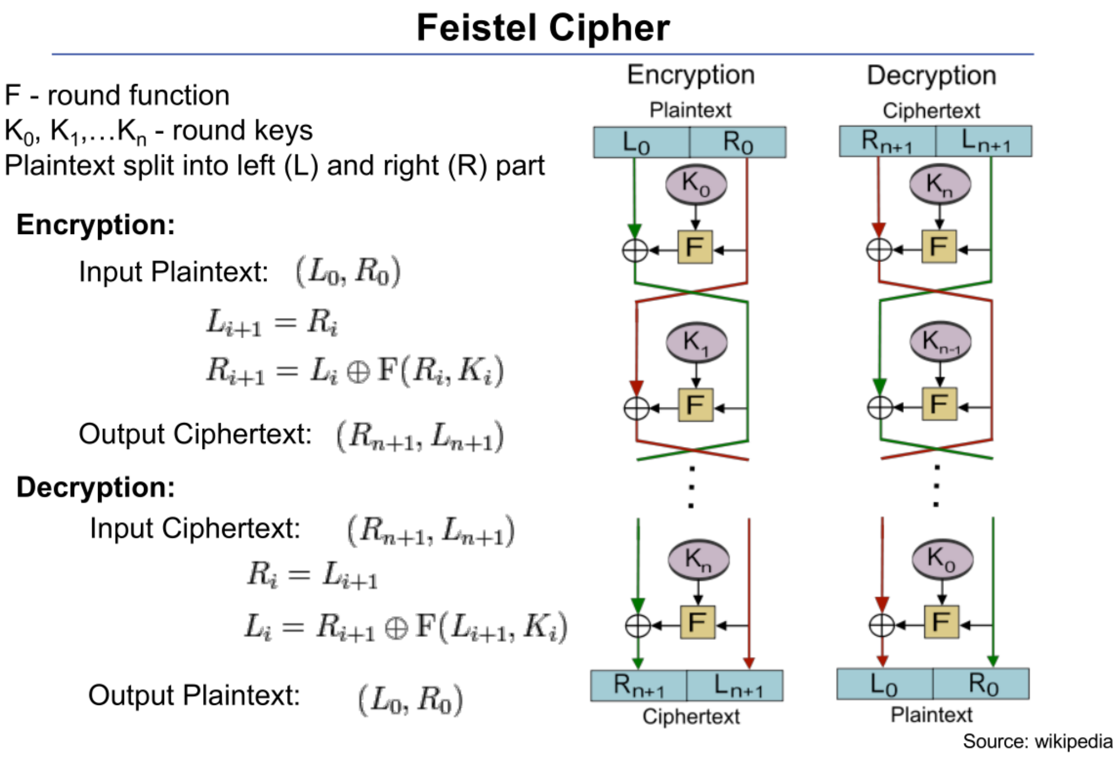
32. RC4: How is the new value S[t] calculated based on S[i] and S[j] in the RC4 stream cipher (after initialization is completed)



```
i=i+1 mod 256              Increase index i
j=(j+S[i]) mod 256         Calculate index j
swap(S[i],S[j])            Swap Bytes
t=(S[i]+S[j]) mod 256      Calculate index t
output S[t]                Output byte for keystream
```

33. What is an improper implementation of RC4, that leads to a known vulnerability in networks?
WEP
→ see Fluhrer-Mantin-Shamir Attack on WEP

34. Draw the functional blocks and the structure of a Feistel cipher



Feistel Cipher

F - round function
$K_0, K_1, \ldots K_n$ - round keys
Plaintext split into left (L) and right (R) part

Encryption:

Input Plaintext: (L_0, R_0)

$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus \mathrm{F}(R_i, K_i)$$

Output Ciphertext: (R_{n+1}, L_{n+1})

Decryption:

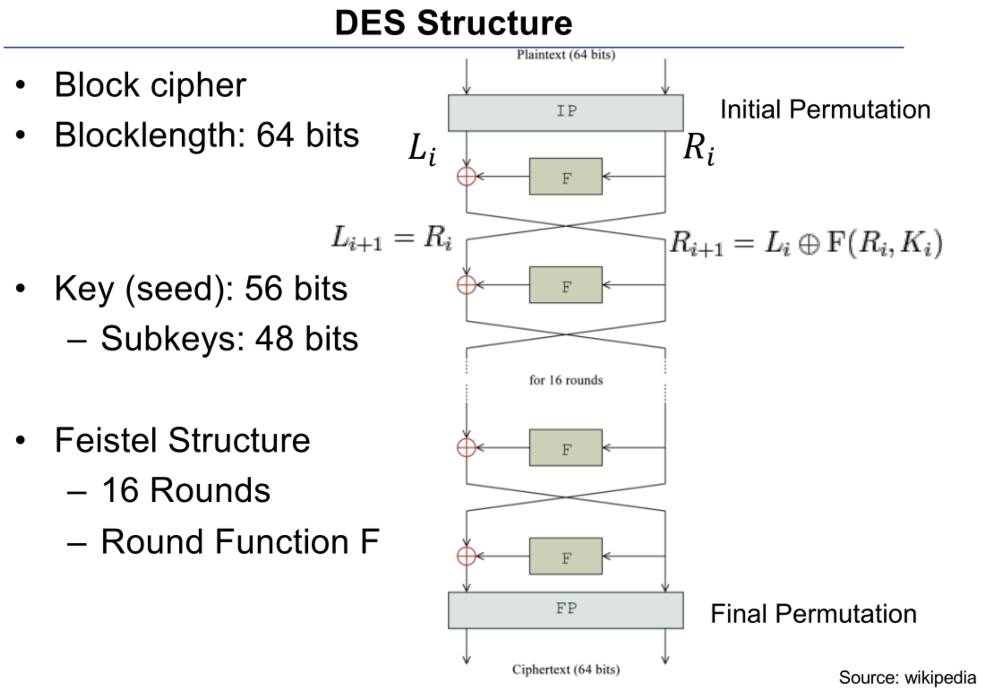
Input Ciphertext: (R_{n+1}, L_{n+1})

$$R_i = L_{i+1}$$
$$L_i = R_{i+1} \oplus \mathrm{F}(L_{i+1}, K_i)$$

Output Plaintext: (L_0, R_0)

Source: wikipedia

35. DES: Which building blocks does DES use?



DES Structure

- Block cipher
- Blocklength: 64 bits
- Key (seed): 56 bits
  - Subkeys: 48 bits
- Feistel Structure
  - 16 Rounds
  - Round Function F

Source: wikipedia

36. 2DES: If E(m,kA) is the encryption function for Single-DES: How does the encryption function for Double DES look like?

$C = E(E(m,k_A),k_B)$

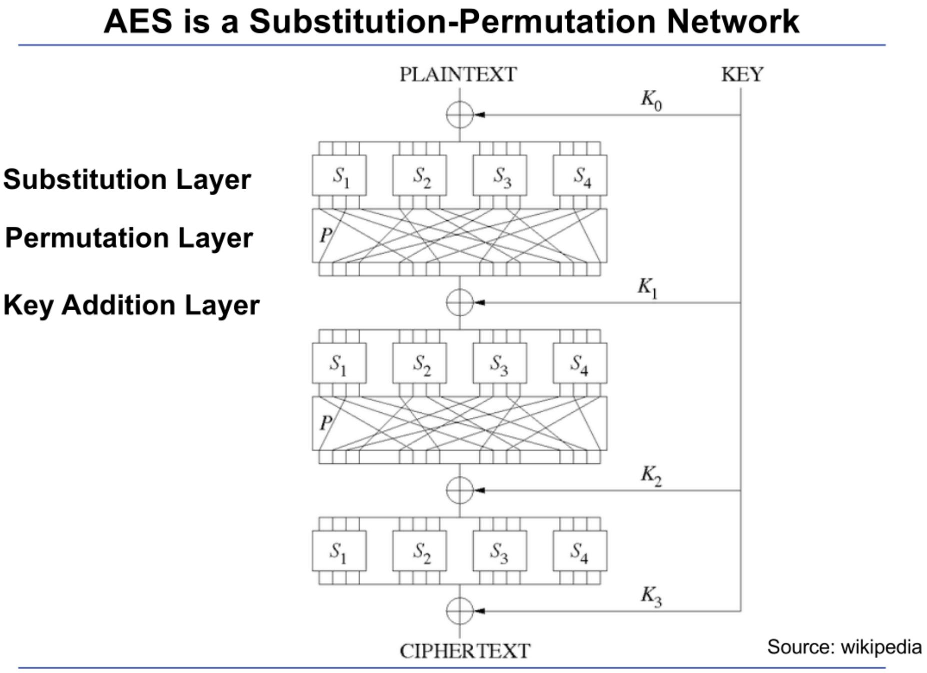
37. 3DES: Why isn't 3DES's encryption function E(E(E(m,k1),k2),k3)?

Because of backwards compatibility.
If $k_A = k_B = k_C$ → single DES

38. AES: What are the 4 operations/steps of the AES cipher? How many rounds are performed?

- SubBytes
  - Substitute bytes in message
- ShiftRows
  - Shift bytes within a row of the block
- MixColumns
  - Multiply columns with matrix
  - Except in final round
- AddRoundKey
  - XOR column with part of round key

Rounds: 10-14 (depends on the key length)



AES is a Substitution-Permutation Network

Source: wikipedia

39. How does Electronic Code Book (ECB) mode work?

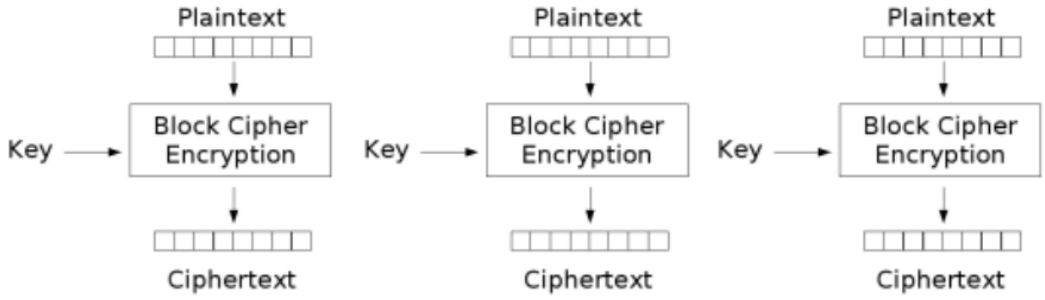
- Message is split into blocks of equal size
- If needed padding
- Each block encrypted independently
- (Problem: equal plaintext generates equal ciphertext)

40. What can be used in an attack of ECB-encrypted messages?

- equal plaintext generates equal ciphertext(???)

41. Name and draw the five most common block cipher modes named in the lecture.

A. Electronic Code Book (ECB)

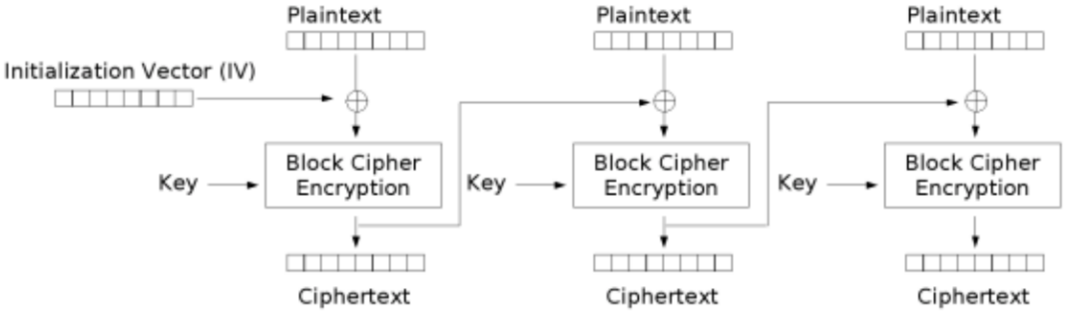


Electronic Codebook (ECB) mode encryption

Source: wikipedia

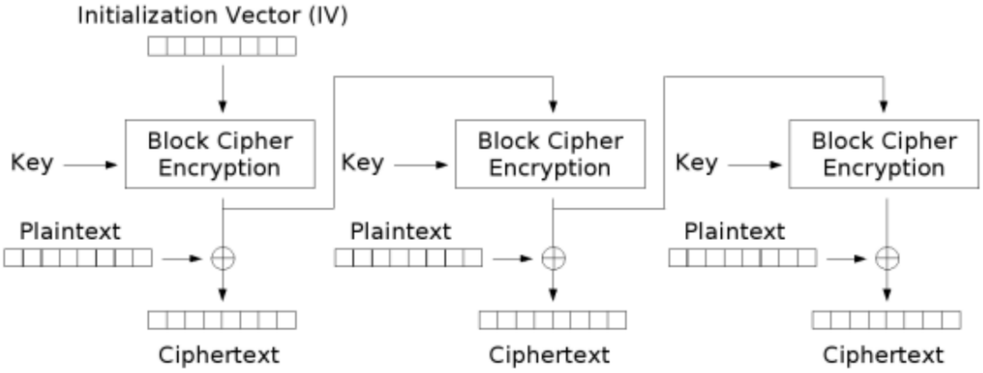
B. Cipher Block Chaining (CBC)

Cipher Block Chaining (CBC)



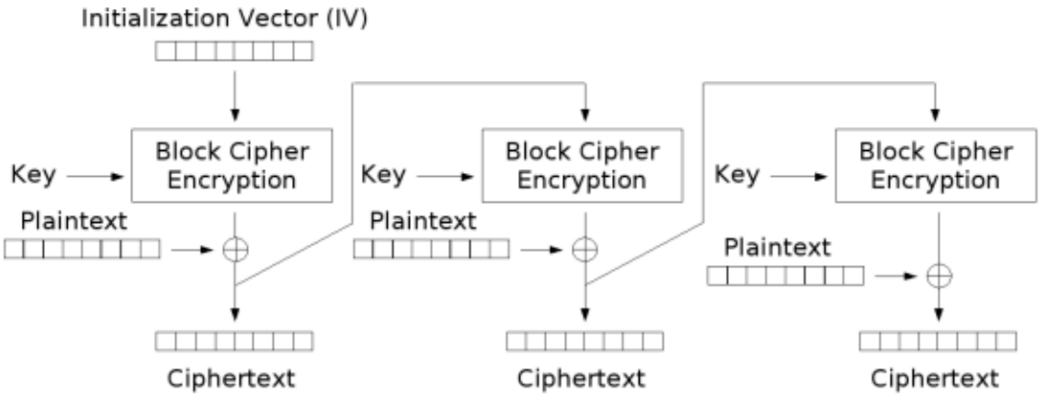
Cipher Block Chaining (CBC) mode encryption

C. Output Feedback (OFB)



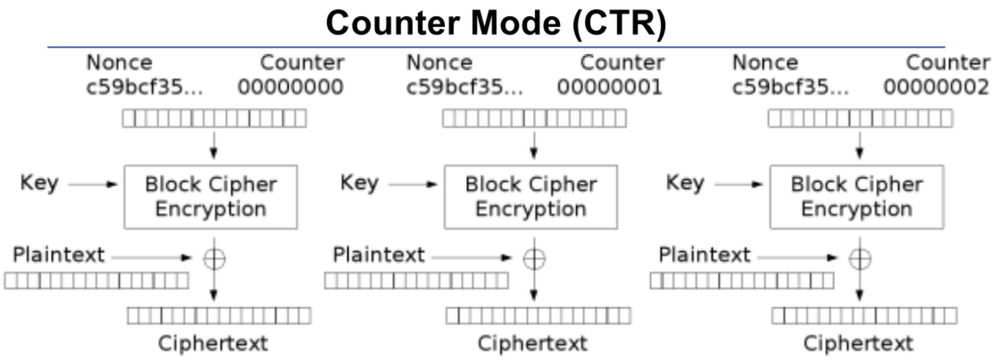
Output Feedback (OFB) mode encryption

D. Cipher Feedback (CFB)



Cipher Feedback (CFB) mode encryption

E. Counter Mode (CTR)



Counter (CTR) mode encryption

42. What are the options for authenticated encryption?

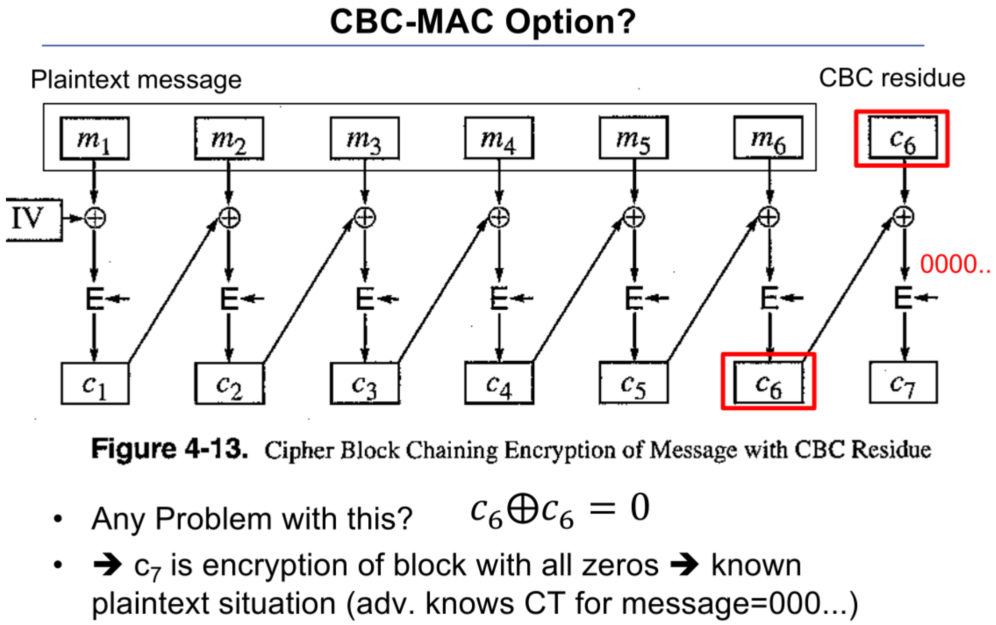
- **Encrypt-and-MAC (=Message Authentication Code)**
  - Encrypt message
  - Calculate MAC from (Plaintext) message
  - → no integrity of Ciphertext, MAC my reveal plaintext info
- **MAC-then-encrypt**
  - Calculate MAC and append to message
  - Encrypt message (with appended MAC)
  - → no integrity of Ciphertext
- **Encrypt-then-MAC**
  - Encrypt message
  - MAC over encrypted message → integrity of Ciphertext
  - → best option, standard method

43. Why isn't a CRC a good Message Authentication Code?

  - CRC is Cyclic Redundancy Check (https://en.wikipedia.org/wiki/Cyclic_redundancy_check)

- CRC does not use key → not suitable

44. What is meant with CBC-MAC? What is the problem associated with it?
    - Uses last block of CBC operation (CBC residue) as MAC
    - Depends on message and key
    - Problems:

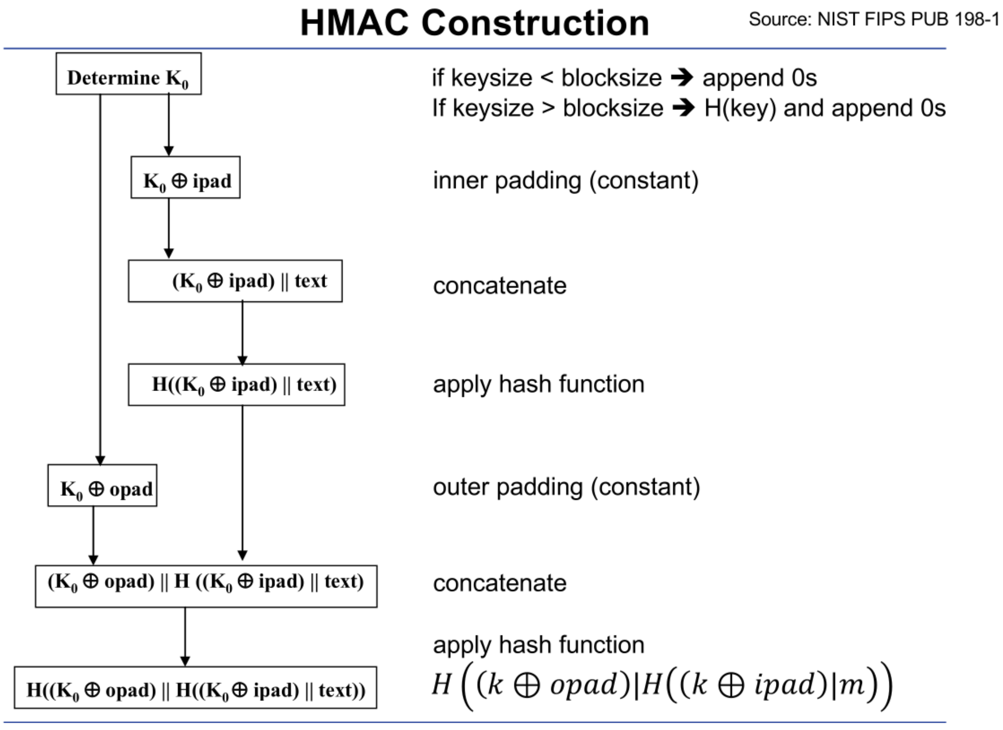


CBC-MAC Option?

Figure 4-13. Cipher Block Chaining Encryption of Message with CBC Residue

- Any Problem with this? $c_6 \oplus c_6 = 0$
- ➔ c_7 is encryption of block with all zeros ➔ known plaintext situation (adv. knows CT for message=000...)

45. How is an HMAC built?



HMAC Construction

Source: NIST FIPS PUB 198-1

Determine K_0 — if keysize < blocksize ➔ append 0s
If keysize > blocksize ➔ H(key) and append 0s

$K_0 \oplus$ ipad — inner padding (constant)

($K_0 \oplus$ ipad) || text — concatenate

H(($K_0 \oplus$ ipad) || text) — apply hash function

$K_0 \oplus$ opad — outer padding (constant)

($K_0 \oplus$ opad) || H (($K_0 \oplus$ ipad) || text) — concatenate

H(($K_0 \oplus$ opad) || H(($K_0 \oplus$ ipad) || text)) — apply hash function

$$H\left((k \oplus opad)|H((k \oplus ipad)|m)\right)$$

46. **Name 5 properties that should be fulfilled by a cryptographic hash function.**

- **Compression**
    - len(h(x)) < len(x)
    - h(x) usually fixed size
- **Efficiency**
    - Easy to compute h(x) for any x
- **One-way**
    - No feasible way to invert hash, i.e. find x for a given y=h(x)
- **Weak collision resistance**
    - Given x and h(x) infeasible to find any y such that h(y)=h(x)
    - Not feasible to modify message without changing the hash
- **Strong collision resistance**
    - Infeasible to find any x and y such that h(y) = h(x)
    - Cannot find any two inputs that hash to the same output

04. Asymmetric cryptography

47. What are private and public keys? What is the relation between them? **When are these used to sign, encrypt, decrypt and verify a signature?**

Sending encrypted message from A to B

- Public key:
    - Public key of B, A (or anyone else) uses it to encrypt the message, so it is public
- Private key:
    - Only B has it and therefor only B can decrypt the message
- Signature:
    - B can sign something with the private key, so A knows, only B is signer
- Relation:
    - IMHO: depends on the used algorithm

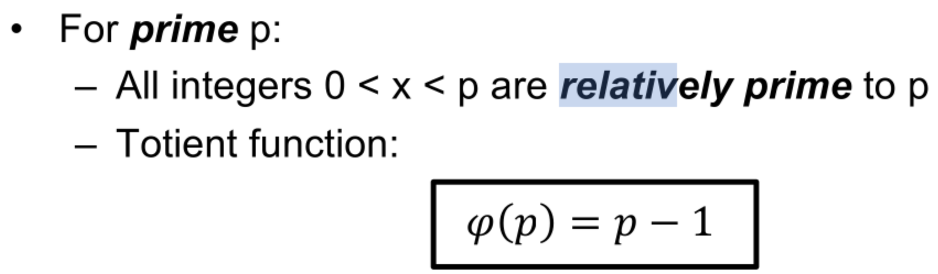
48. How can authentication be performed via asymmetric cryptography?
    - Do not use the same key for authentication and for encryption
    - Use initial key for authentication
    - Agree on a new key for encryption and data integrity
    - Agree on a new key for each session (session key)
        - Limit the data encrypted with one key
        - Limit damage if key is compromised

49. What is meant with the discrete logarithm problem?

Finding the correct a in the expression A = g^a mod p for a given g, p and A is hard.

50. What function can be used to find out how many numbers 1 <= x <= n are relatively prime to n? Calculate this function for a given n and for a product of two factors.

- Euler's Totient Function for prime p:



- For ***prime*** p:
  - All integers 0 < x < p are ***relatively prime*** to p
  - Totient function:

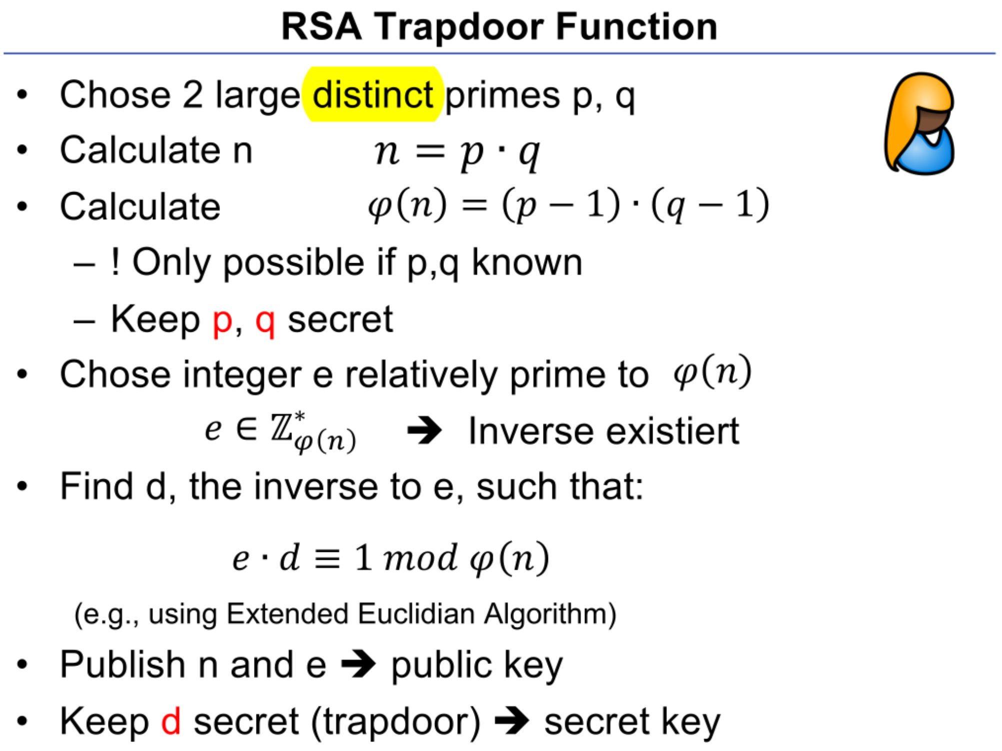
$$\boxed{\varphi(p) = p - 1}$$

- For integers n = p*q with primes p, q:

$$\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$$

$$\boxed{\varphi(n) = (p-1) \cdot (q-1)}$$

51. How does the Rivest-Shamir-Adleman trapdoor function work?



RSA Trapdoor Function

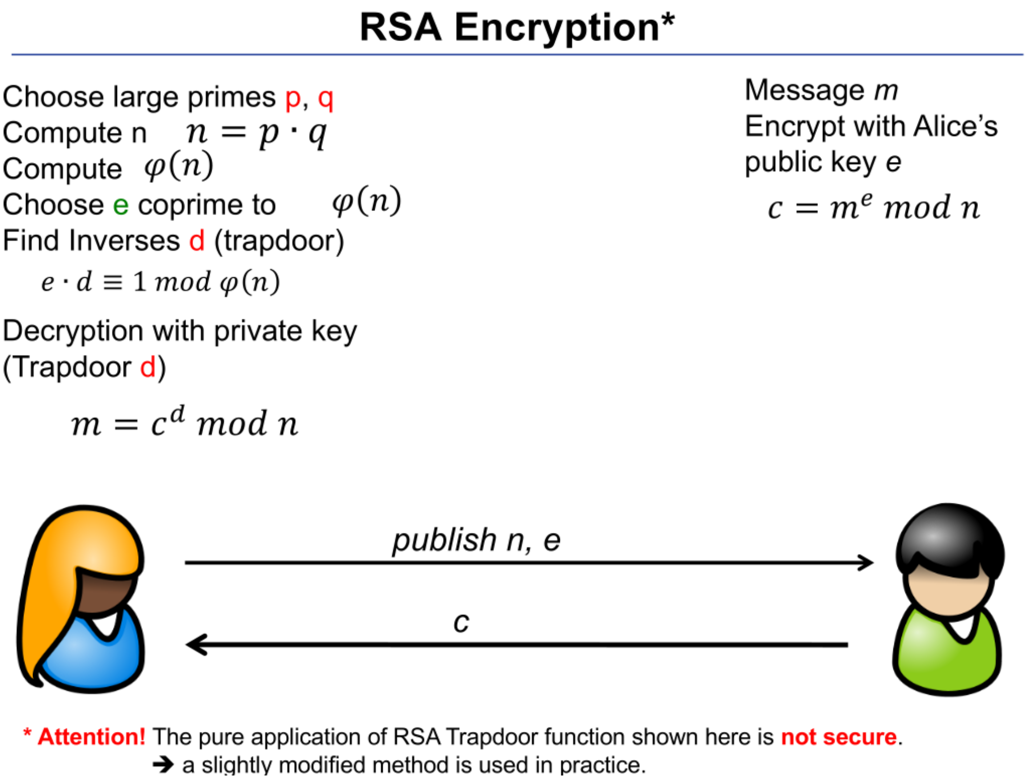
- Chose 2 large distinct primes p, q
- Calculate n $\quad n = p \cdot q$
- Calculate $\quad \varphi(n) = (p-1) \cdot (q-1)$
  - ! Only possible if p,q known
  - Keep p, q secret
- Chose integer e relatively prime to $\varphi(n)$

  $e \in \mathbb{Z}^*_{\varphi(n)}$ ➔ Inverse existiert
- Find d, the inverse to e, such that:

$$e \cdot d \equiv 1 \; mod \; \varphi(n)$$

(e.g., using Extended Euclidian Algorithm)
- Publish n and e ➔ public key
- Keep d secret (trapdoor) ➔ secret key

52. RSA: How are encryption and decryption functions for RSA?



RSA Encryption*

Choose large primes p, q

Compute n $n = p \cdot q$

Compute $\varphi(n)$

Choose e coprime to $\varphi(n)$

Find Inverses d (trapdoor)

$$e \cdot d \equiv 1 \; mod \; \varphi(n)$$

Decryption with private key (Trapdoor d)

$$m = c^d \; mod \; n$$

Message *m*

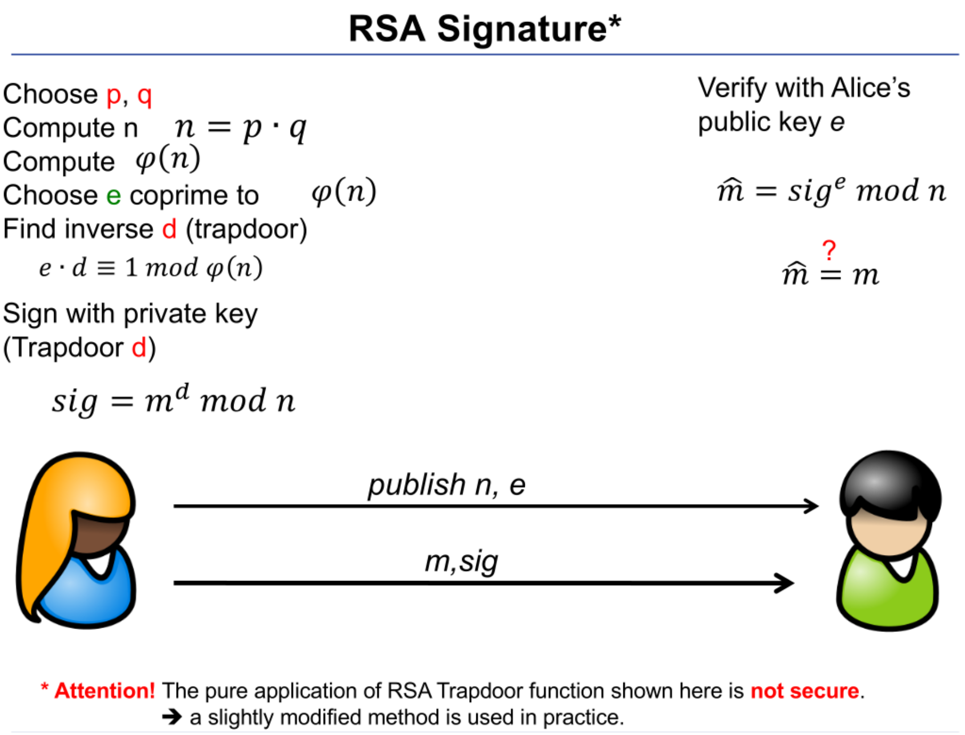
Encrypt with Alice's public key *e*

$$c = m^e \; mod \; n$$

* **Attention!** The pure application of RSA Trapdoor function shown here is **not secure**.

➔ a slightly modified method is used in practice.

53. RSA: How is a digital signature generated based on RSA?



RSA Signature*

Choose p, q

Compute n $n = p \cdot q$

Compute $\varphi(n)$

Choose e coprime to $\varphi(n)$

Find inverse d (trapdoor)

$$e \cdot d \equiv 1 \; mod \; \varphi(n)$$

Sign with private key (Trapdoor d)

$$sig = m^d \; mod \; n$$

Verify with Alice's public key *e*

$$\hat{m} = sig^e \; mod \; n$$

$$\hat{m} \overset{?}{=} m$$

* **Attention!** The pure application of RSA Trapdoor function shown here is **not secure**.

➔ a slightly modified method is used in practice.

54. What is a Forward Search attack?

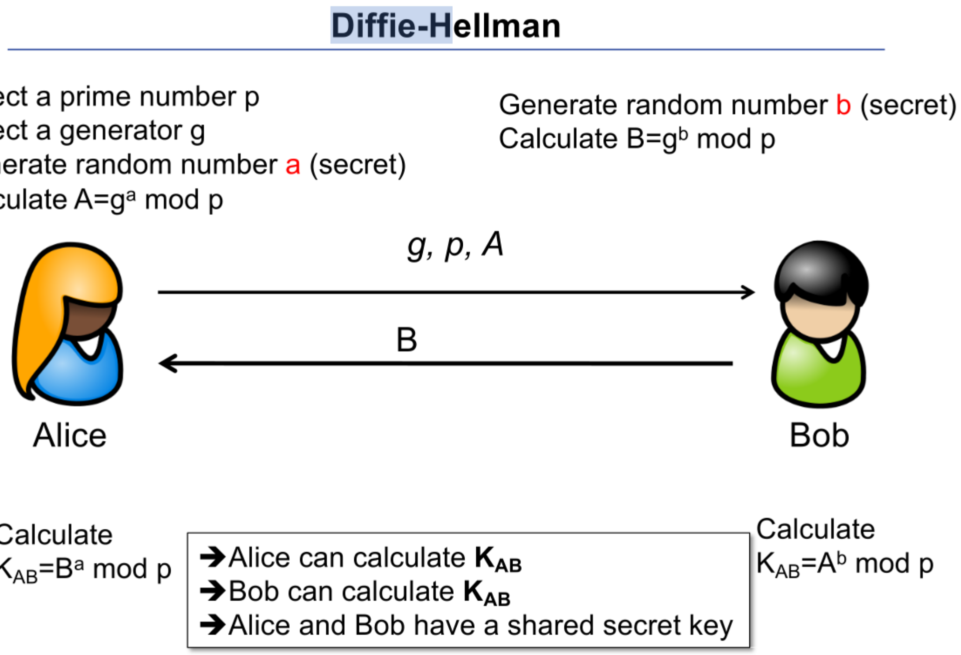
- Attacker guesses message and compares with pre-generated ciphertext

$$m_1 = "YES"$$
$$m_2 = "NO"$$
$$c_1 = m_1^e \bmod n$$
$$c_2 = m_2^e \bmod n$$

$$Check\ if \quad c = c_1 \quad or \quad c = c_2$$

55. Why do we need to introduce a random padding in messages encrypted with public-key cryptography?
    Same message produces the same ciphertext!

56. Sketch the Diffie-Hellman key exchange.



Diffie-Hellman

Select a prime number p
Select a generator g
Generate random number a (secret)
Calculate A=g^a mod p

Generate random number b (secret)
Calculate B=g^b mod p

Calculate
K_{AB}=B^a mod p

➔Alice can calculate **K_{AB}**
➔Bob can calculate **K_{AB}**
➔Alice and Bob have a shared secret key

Calculate
K_{AB}=A^b mod p

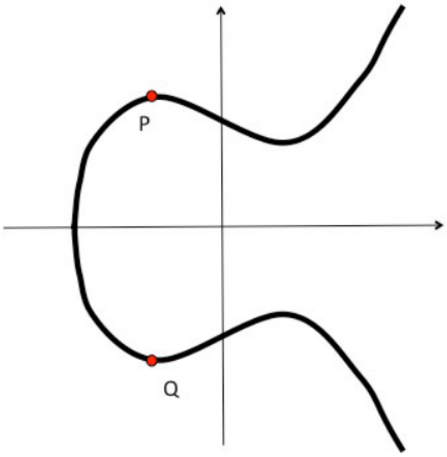
57. What is perfect forward secrecy?

- Prevent adversary from decrypting (previously recorded) messages if he gets access to the longterm key
- → use session keys
- Prevent that session key gets known

58. Can you prove that a message signed from Bob (RSA) is valid (e.g. at court)?

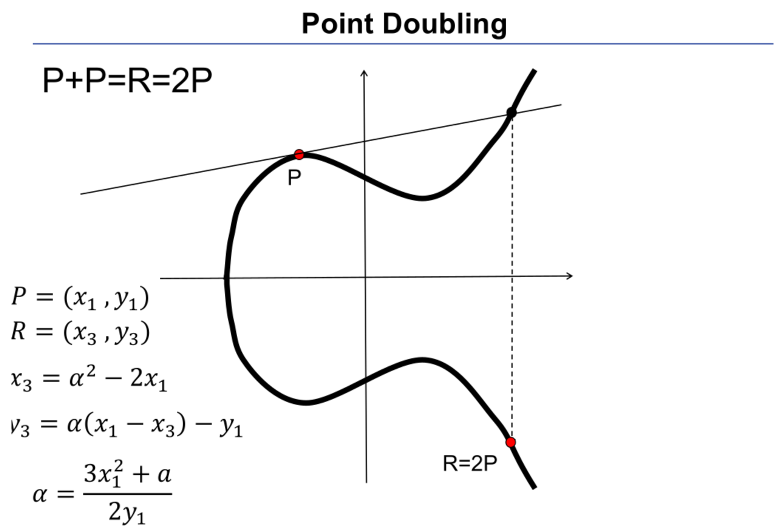
   a. Don’t know, but I would guess: YES!

59. **What is the difference between a message authentication code and a digital signature?**
https://crypto.stackexchange.com/questions/5646/what-are-the-differences-between-a-digital-signature-a-mac-and-a-hash
    - **MAC:**
        - Symmetric key
    - **Digital Signature**
        - Asymmetric key
60. ECC vs RSA, what are the advantages of using ECC in place of RSA?
Shorter key length for same security level
61. **ECC: What is the result of an addition of the points P and Q if elliptic curve arithmetic is used? What about P+P?**



In this example:

- P+Q is the identity element (infinity, 0)
- P+P will lead to a new Point R



Point Doubling

P+P=R=2P

$P = (x_1 , y_1)$
$R = (x_3 , y_3)$
$x_3 = \alpha^2 - 2x_1$
$y_3 = \alpha(x_1 - x_3) - y_1$
$\alpha = \dfrac{3x_1^2 + a}{2y_1}$

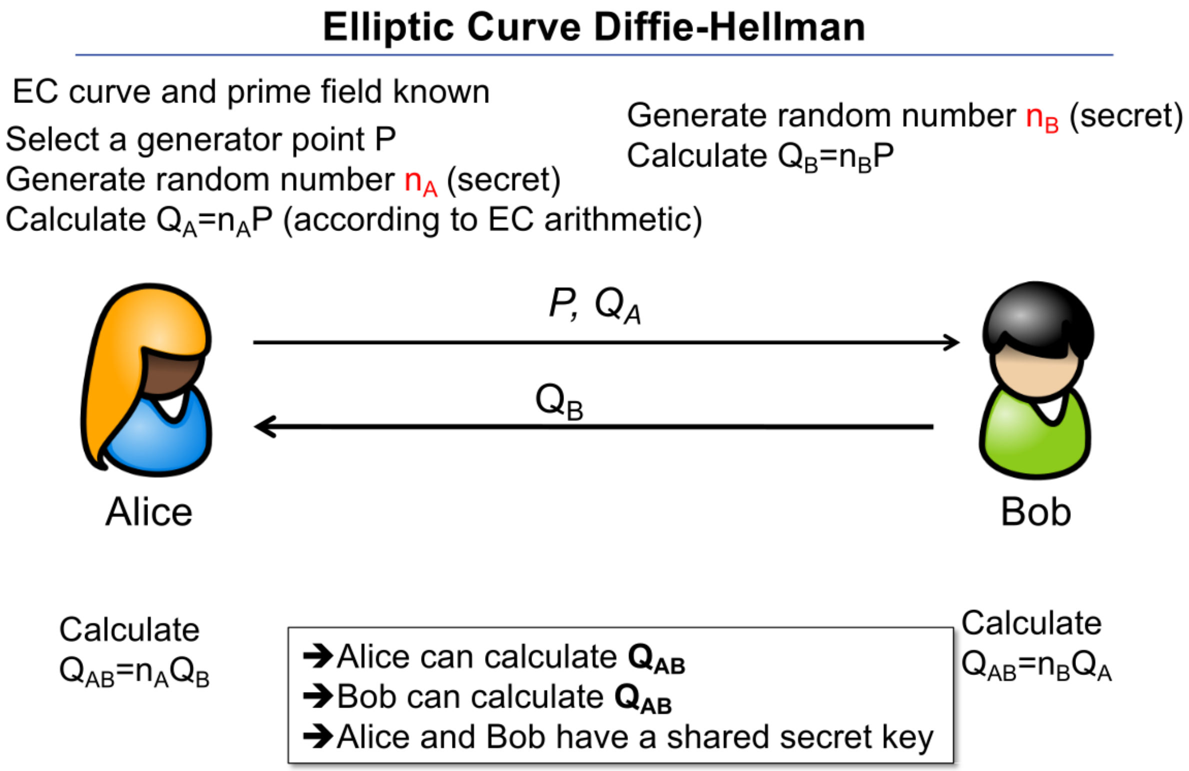
62. ECC: What is used as a generator in elliptic curve encryption?

- Elliptic curve is a graph with:
  - $y^2=x^3+ax+b$
  - $4a^3+27b^2 \neq 0$

63. ECC: What are public and private parameters of ECC?

    Not on slides - only for D-H

64. ECC: Sketch the Elliptic-Curves Diffie-Hellman key exchange.



Elliptic Curve Diffie-Hellman

EC curve and prime field known

Select a generator point P
Generate random number n_A (secret)
Calculate $Q_A=n_AP$ (according to EC arithmetic)

Generate random number n_B (secret)
Calculate $Q_B=n_BP$

Calculate
$Q_{AB}=n_AQ_B$

Calculate
$Q_{AB}=n_BQ_A$

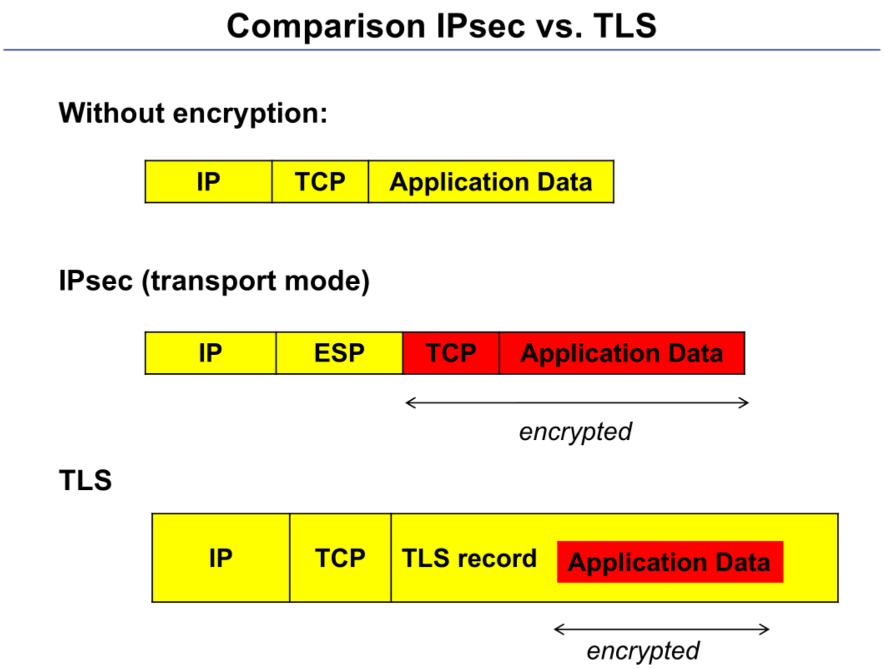
➔Alice can calculate $\mathbf{Q_{AB}}$
➔Bob can calculate $\mathbf{Q_{AB}}$
➔Alice and Bob have a shared secret key

05 Anomaly Detection

65. **IPSec Authentication Header (AH) provides:**
    a. **( ) Confidentiality only**
    b. **(X)Integrity only**
    c. **( ) both Confidentiality and Integrity**
66. What are the three different modes of use of IPsec?
    - Endpoint-to-Endpoint Transport Mode
    - Security Gateway to Security Gateway Tunnel Mode
    - Endpoint to Security Gateway Tunnel Mode (VPN)
67. What is the Internet Key Exchange and what is its relation with IPsec?
    - Goal: Establish a shared state between sources and destination
        - Which services are provided
        - Which cryptographic algorithms are used
        - Which keys are used as input
        - → Establish IKE Security Association (SA)
    - Mutual authentication
        - Know identity of the communication partner
    - Establish keying material to be used for IPSec
        - Encryption
        - Integrity Check
68. **In TLS: (Multiple choice)**
    a. **(X) The TCP Port is not encrypted**
    b. **(X) Client auth is optional**
    c. **(X) DH can be used for key exchange**
69. What are the main differences between IPsec and TLS?

    IPSec:
    - Network layer
    - Secure connection between devices
    - Establishment of security association
    - Example Usage: VPN

    TLS:
    - On top of transport layer (usually TCP)
    - Secure connection between applications
    - Relies on be-directional reliable transport layer
    - Example Usage: HTTPS



Comparison IPsec vs. TLS

Without encryption:

IPsec (transport mode)

TLS

70. What is a traffic flow?

    Maybe the way the traffic uses from A to B?

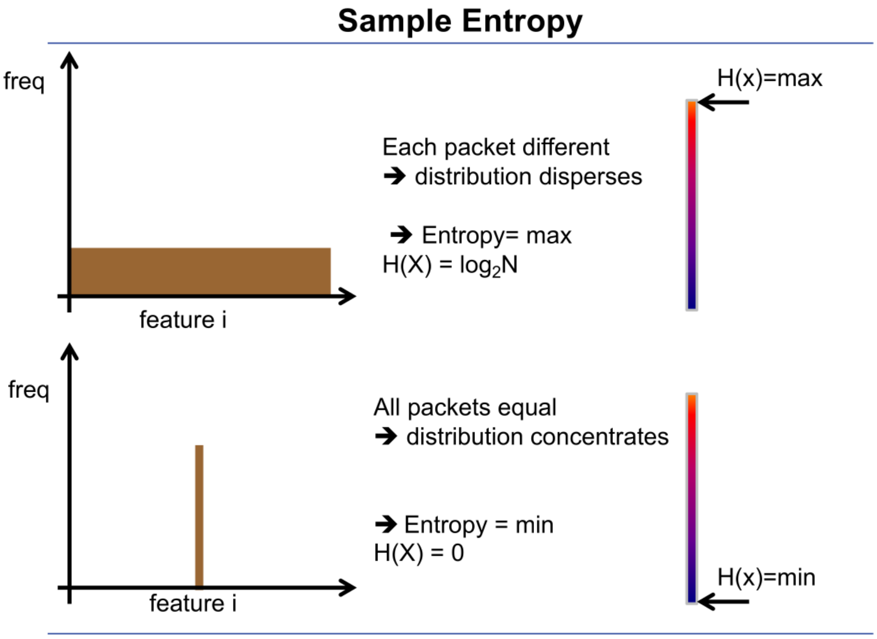
71. What are the four steps for traffic aggregation?

    Maybe
    - Timestamping
    - Selection
    - Classification
    - Aggregation

72. **What is the darkspace?**

    IP addresses announced by routing but no hosts attached

73. **What is entropy? Distinguish between two samples, which one has higher entropy.**
    - Measures information content of a message
        - Depends on probability of event
    - Sample Entropy
        - Describe histogram by entropy value (estimation)
        - Capture degree of dispersion or concentration



Sample Entropy

Each packet different
➔ distribution disperses

➔ Entropy= max
$H(X) = \log_2 N$

All packets equal
➔ distribution concentrates

➔ Entropy = min
$H(X) = 0$

74. **How can entropy values be used to detect attacks?**

Feinstein/Schnackenberg 2003

a. Detection of DDoS attacks based on source IP entropy

Lakhina et al 2005

b. Detection of scanning, DDoS, outages based on combinations of entropy from addresses and ports

75. What are the two detection techniques for attacks? What are their pros and cons?

- Signature based Detection
  - Pro:
    - Simple operation (comparison to signature)
    - Few false positives
  - Con
    - Collection of signatures
    - Signature updates required
    - Fails for unknown attacks (Zero-Day events)
- Anomaly Detection
  - Pro:
    - Detection of novel attacks
    - No signatures required
  - Con:
    - Model and training required
    - May be trained by attacker
    - Anomaly not always malicious

    - False positives

76. **What is a point anomaly?** Contextual anomaly? Collective anomaly?

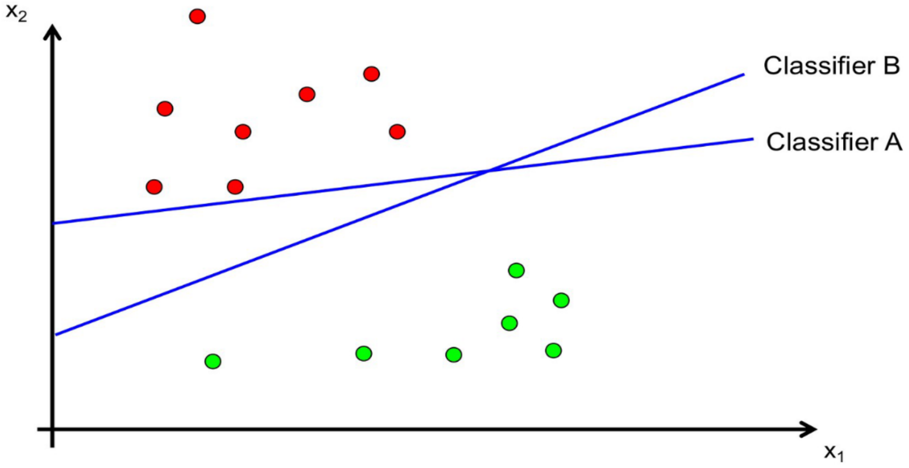
    Point anomalies: A single instance of data is anomalous if it's too far off from the rest. *Business use case:* Detecting credit card fraud based on "amount spent."

    Contextual anomalies: The abnormality is context specific. This type of anomaly is common in time-series data. *Business use case:* Spending $100 on food every day during the holiday season is normal, but may be odd otherwise.

    Collective anomalies: A set of data instances collectively helps in detecting anomalies. *Business use case:* Someone is trying to copy data form a remote machine to a local host unexpectedly, an anomaly that would be flagged as a potential cyber attack.

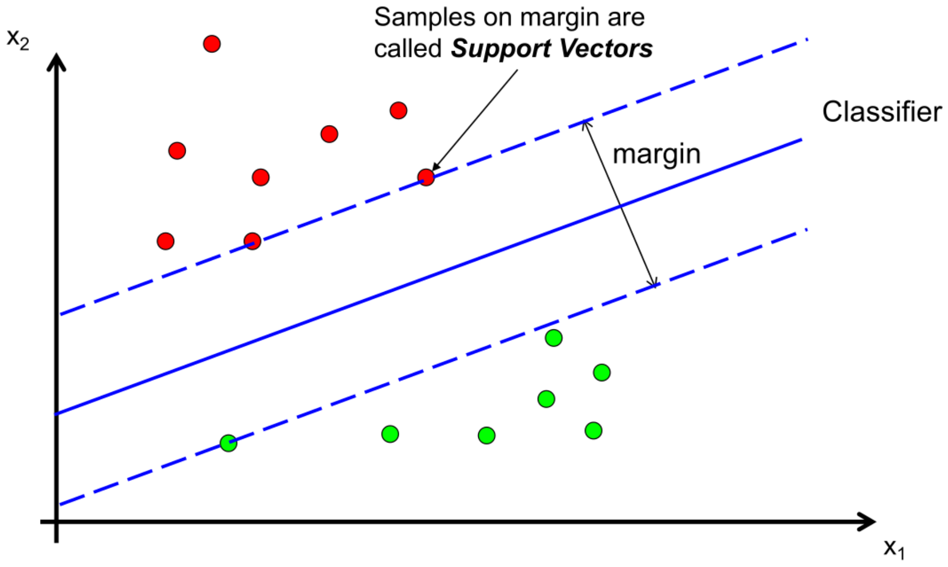
    Source: https://blogs.oracle.com/ai-and-datascience/post/introduction-to-anomaly-detection

77. **What is the purpose of Support Vector Machines (SVMs)?**
    Data classification
78. **What can be done if you only have a technique to learn a linear classifier but the data is not linear separable?**
    Transform points to higher dimension
79. **Which classifier is better? How do we know? Which points are the support vectors?**



Classifier B, because the margin is bigger compared to classifier A (margin should be maximized) The closest points to the classifier are the support vectors

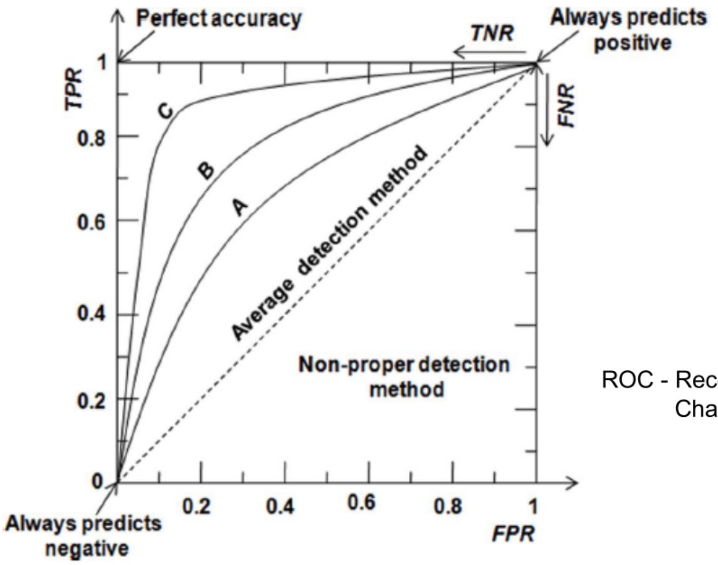
Support Vector Machines (SVM)



➔ Maximize the margin

80. What is meant with Area under the ROC curve?

Area Under ROC Curve (AUC)



ROC - Receiver Operating Characteristic

The bigger the area under the ideal curve, the better the detection method. So C would be awesome, B still good, A questionable and everything else BAD.