Frage (2Pkt)

IPsec: Which functions does an IPsec ESP header support? Mark the supported functions.

[ ] None. Neither Confidentiality nor Integrity.

[ ] Confidentiality and Integrity

[ ] Integrity, but no Confidentiality

[ ] Confidentiality, but no Integrity

> false, true, false, false

Frage(2Pkt)

The following text has been encrypted with a Cesar cipher with k=3. Decrypt the text.

FRUUHFW

Antwort:

> CORRECT

Frage (4Pkt)

Stream Ciphers: You use a pseudo random generator (PRG) to generate a pseudo random sequence G(s). To check the quality of the PRG you use a statistical test A. For the test you have the following probabilities:

P(A(R) = 1) = 0.9
Probability that the statistical test returns 1 if applied to a real random sequence R
P(A(G(s)) = 1) = 0.9
Probability that the same statistical test returns 1 if applied to your pseudo random sequence G(s)
Notation: As decimal separator (if needed) use a point if you use TUWEL in English and a comma if you use TUWEL in
German.

a) Calculate the Advantage (just provide the result).

Adv(A,G(s)) =

> 0

b) Is your PRG a good pseudo random generator?

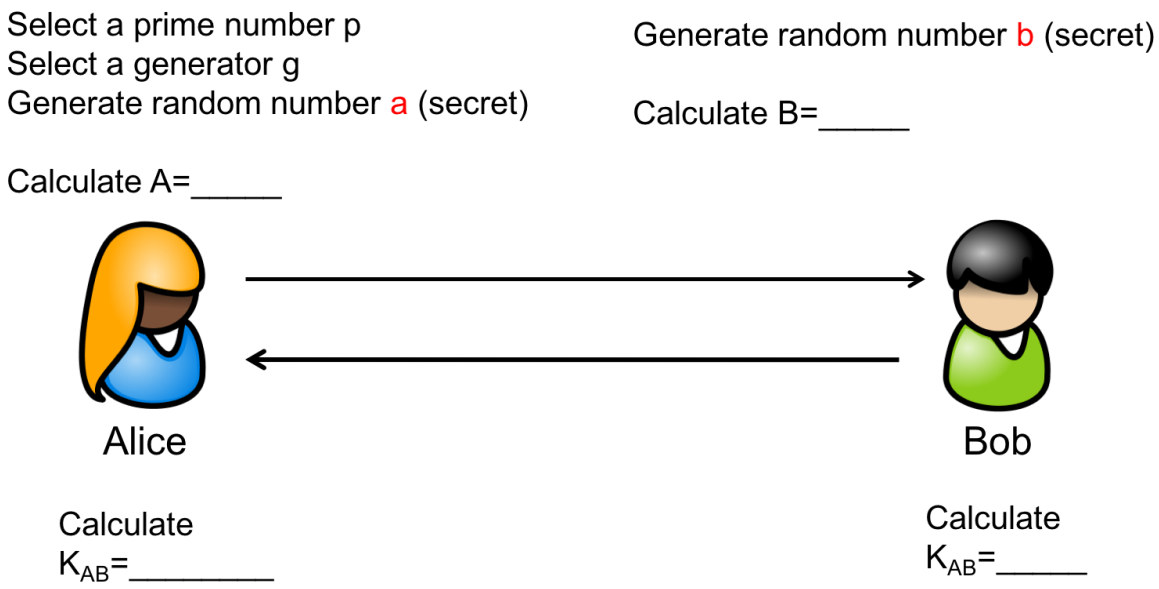
> Yes

Frage (6Pkt)

DH Key Exchange: Given is the Diffie-Hellman Key Exchange.

1. How do Alice and Bob calculate A and B?
2. Which values do they exchange? (who sends what to whom?)
3. How do they calculate the key? (show the key calculation for each of them)

General Remarks on Notation: Use _ to indicate a subscript (e.g., write x_1 for x 1). Use ^ to indicate a superscript (e.g., write x^2 for x 2). For multiplication use the * sign with blanks (e.g., x * y).



Answer for Question 1:
A=

> g^a mod p

B =

> g^b mod p

Answer for Question 2:

Alice sends to Bob:

> g,p,A

Bob sends to Alice:

> B

Answer for Question 3:

Alice calculates the key K_AB =

> B^a mod p

Bob calculates the key K_AB =

> A^b mod p

Frage (2Pkt)

DES: The DES Encryption for a message m into a ciphertext c with key k1 is defined as c=E(m,k1). The DES decryption is
defined as m=D(c,k1).
Double DES (2DES) encryption with the keys k1, k2 is defined as c=E(E(m,k1),k2)
Show the definition of the Triple DES (3DES) encryption with the keys k1, k2, k3. (start the equation with c=)

> c=E(D(E(m,k1),k2),k3)

Frage (4Pkt)

Bob wants to use RSA to send an encrypted message to Alice. He knows her public key e and the modulus n.
a) Show which equation Bob uses to calculate the ciphertext c from the message m.
b) Show which equation Alice uses to calculate the message m from the ciphertext c.
General Remarks on Notation: Use _ to indicate a subscript (e.g., write x_1 for x 1). Use ^ to indicate a superscript (e.g.,
write x^2 for x 2). For multiplication use the * sign with blanks (e.g., x * y).

a) Bob calculates the ciphertext c =

> m^e mod n

b) Alice calculates the message m =

> c^d mod n

Frage (2Pkt)

Modern ciphers: Which of the following statements are true?

[ ] The Advanced Encryption Standard (AES) is a block cipher.

[ ] The Data Encryption Standard (DES) is a block cipher.

[ ] The Data Encryption Standard (DES) is based on a Feistel cipher.

[ ] The Advanced Encryption Standard (AES) is based on a Feistel cipher.

> true, true, true, false

Frage (2Pkt)

Security: Alice and Bob communicate with asymmetric cryptography. Which key(s) does Alice have? Select all key(s) that she
knows.

[ ] Bob's private key

[ ] Bob's public key

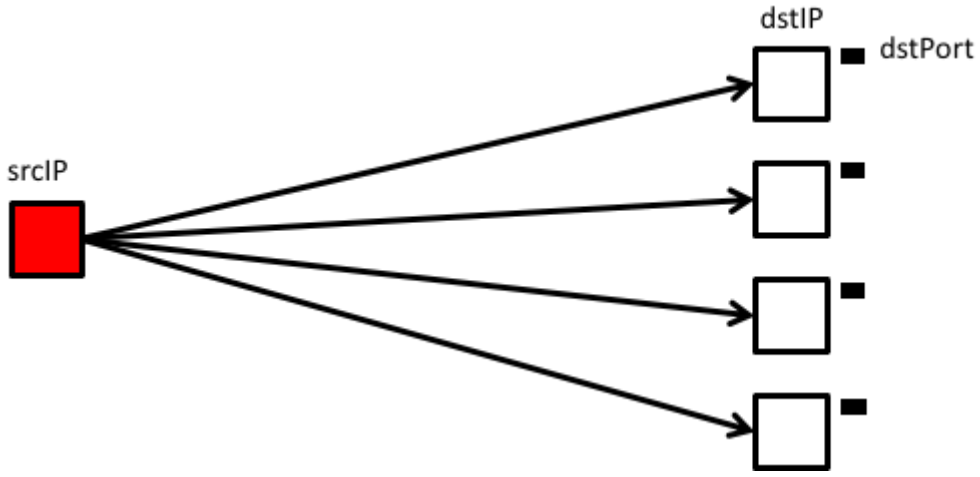
[ ] Alice's public key

[ ] Alice's private key

> false, true, true, true

Frage (2Pkt)

Entropy: You observe a horizontal scan (to one port and many destinations) and look at the distributions of the two features:
destination IP (dstIP) and destination port (dstPort). What can you say about the entropy of the distributions?



[ ] The entropy of the distribution of destination IP addresses is low.

[ ] The entropy of the distribution of destination ports is low.

[ ] The entropy of the distribution of destination IP addresses is high.

[ ] The entropy of the distribution of destination ports is high.

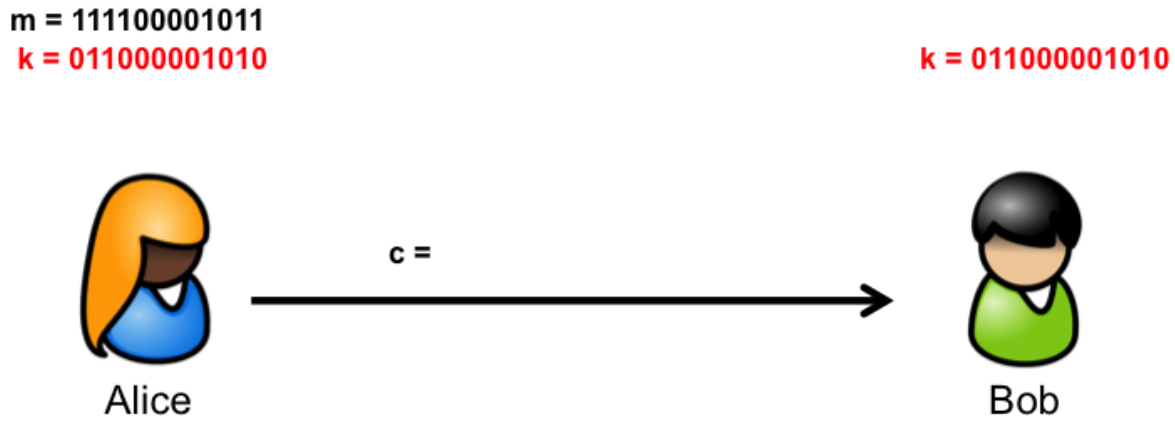
> false, true, true, false

Frage (4Pkt)

One Time Pad: Alice wants to use a One Time Pad with key k=011000001010

to send the message m= 111100001011 to Bob.

1. Which operation is used?
2. How does the resulting ciphertext c look like?



Operation used:

> xor

Ciphertext:

> 100100000001

Frage (2Pkt)

RSA: In RSA which values need to remain secret?

[ ] The private key d.

[ ] The public key e.

[ ] The prime numbers p and q.

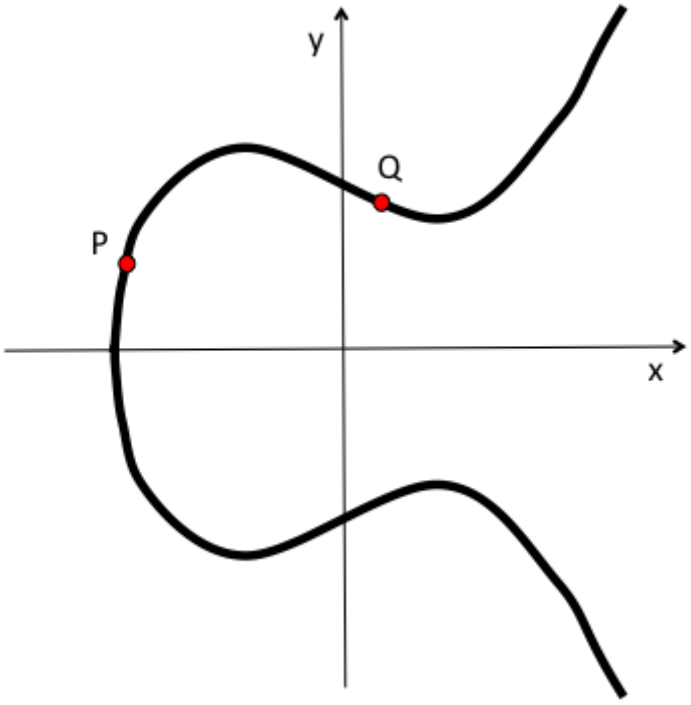
[ ] The value of n.

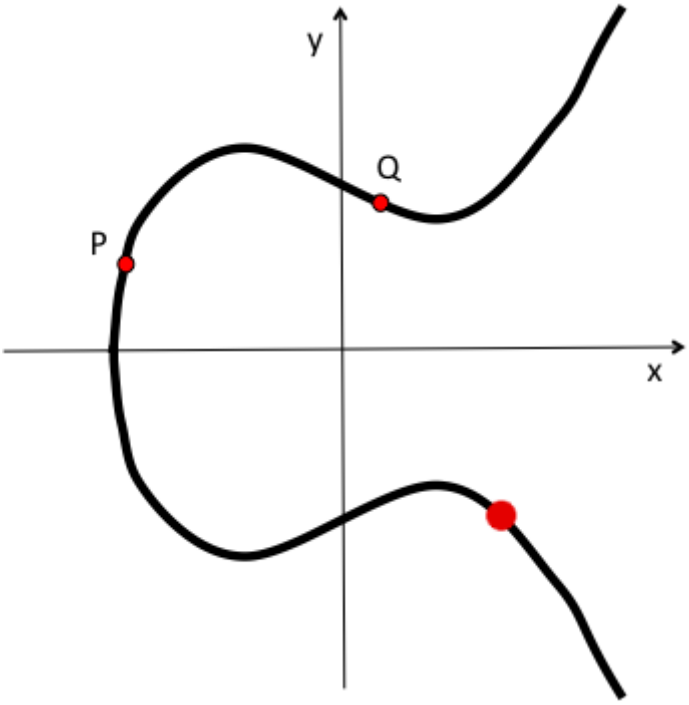
[ ] The value of φ(n).

> true, false, true, false, true

Frage (4Pkt)

What is the result of an addition of the point P with the point Q if elliptic curve arithmetic is used?
Show the resulting point
R=P+Q in the graph below by moving it to the correct position.





Frage (2Pkt)

Darkspace traffic: Which statement(s) are true about darkspace traffic?

[ ] You may see TCP SYN-ACK packets in the darkspace.

[ ] You may see TCP SYN packets in the darkspace.

[ ] You may see UDP packets in the darkspace.

[ ] You may see ICMP packets in the darkspace.

> true, true, true, true

Frage (2Pkt)

Security protocols: Which of the following statements are true?

[ ] When you use IPsec encryption in transport mode, then also the TCP header is encrypted.

[ ] When you use TLS encryption, then also the TCP header is encrypted.

[ ] When you use IPsec encryption in tunnel mode, then also the TCP header is encrypted.

> true, false, true