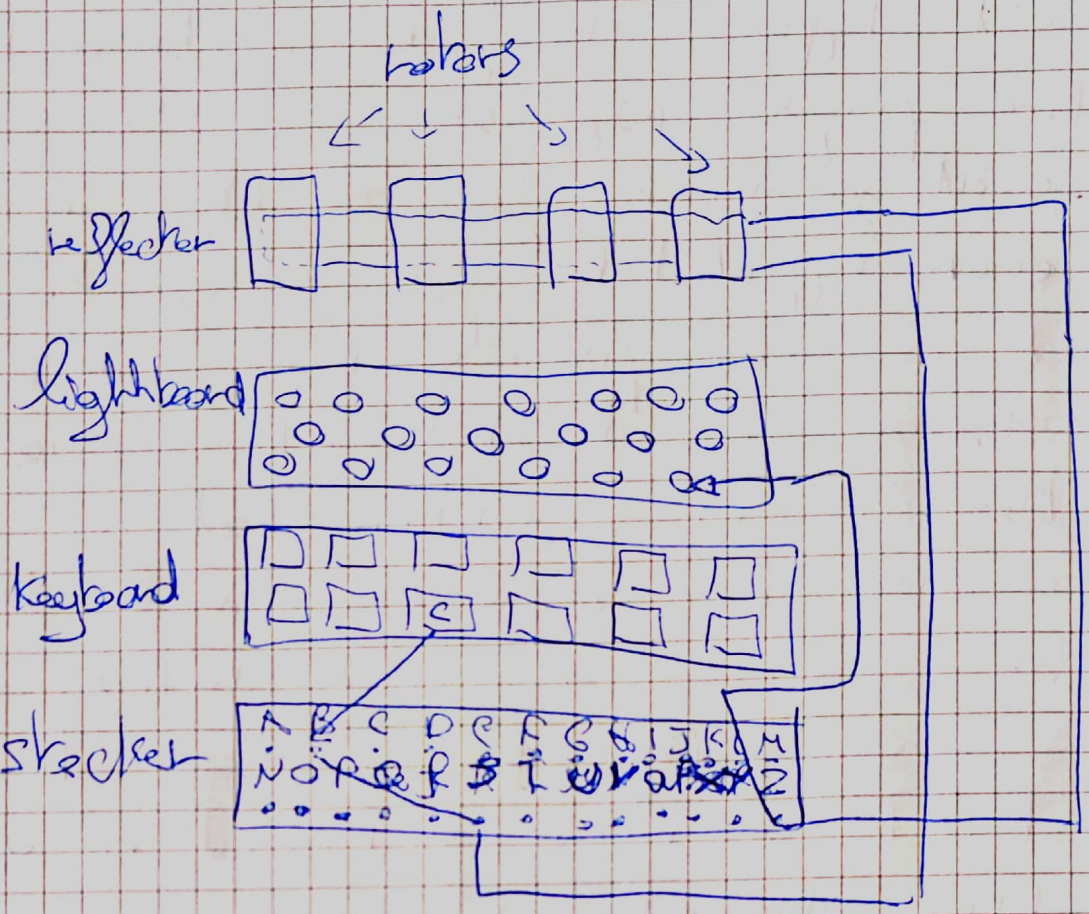
1a)



1b) If the Germans learned that their system had been broken, they could have used that information as an advantage to counter attacks. The Germans were known to use very fast "blitzkrieg" attacks. The German could have sent a few messages that they were sending one of these attacks somewhere while actually invading somewhere else. Such a message could not have been ignored and the Allies would have moved most of their troops to a wrong location.

1c) I can see multiple reasons why that could happen. The first one being that the people responsible for the cipher feared for their life and the issue was never reported to upper management.
It is also possible that when the Germans realised their system was broken they either had not enough resources to completely implement a new system or they started implementing a new system but never got to finish it. Thus they continued to use their original system.

2a) Kerckhoff's principle is the idea that a chyptography system should remain secure when its mech-anisms are public and only the keys remain private.

2b) A5/1, a stream cipher for GSM communication broke the principles by keeping the algorithm private. It was reverse engineered and it is possible to find the key by analysing the output. Another example is the

German enigma cipher.

2) The mechanism(s) of a cryptosystem should be considered public knowledge while the key(s) should be kept private.

3) The key is 4. The plaintext is YOUARETERMINATED.

4a)

k	0	r	:	0	1	1	0	1	1	1	->	1	0	0
r	0	h	:	0	1	0	0	0	1	1	->	0	1	1
l	1	r	:	1	1	1	0	1	0	1	->	0	1	0
k	0	l	:	1	0	0	0	1	0	0	->	1	1	0
e	0	l	:	0	0	0	0	1	0	0	->	1	0	0

Key : 100 011 010 110 111 100

4b)

k	0	r	:	0	1	1	0	1	1	1	->	1	0	0
r	0	l	:	0	1	0	0	1	0	0	->	0	0	0
l	1	l	:	1	1	1	0	1	0	0	->	0	1	1
k	0	e	:	0	1	1	0	0	0	0	->	0	1	1
e	0	r	:	0	0	0	0	1	0	1	->	1	0	1

Key : 100 000 011 000 011 101

5a) Using the 3 possible bit output and the 3 bit we find that x steps 6 out of the 8 possible values for xyz. Thus the value is 3/4.

5b) For the same reason as 5.a., Y steps on average 3/4.

6a) L_0 , R_0

$L_1 = R_0$

$R_1 = L_0 \oplus F(R_1, K_1)$

$= L_0$

$L_1 = R_0$

$R_1 = L_0$

$L_2 = L_0$

$R_2 = R_0$

$L_3 = R_0$

$R_3 = L_0$

$L_4 = L_0$

$R_4 = R_0$ ← réponse

6b) $F(R_{i-1}, K_i) = R_{i-1}$

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus F$

$L_0 , R_0 .$

$L_1 = R_0$

$R_1 = L_0 \oplus R_0$

$L_2 = L_0 \oplus R_0$

$R_2 = R_0 \oplus L_0 \oplus R_0 = \underline{\underline{L_0}}$

$L_3 = L_0$

$R_3 = L_0 \oplus R_0 \oplus L_0 = \underline{\underline{R_0}}$

$L_4 = R_0$

$R_4 = L_0 \oplus R_0$

↑ réponse

6c)

$L_i = R_{i-1}$

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

$F(R_{i-1}, K_i) = K_i$

L_0, R_0

$L_1 = R_0$

$R_1 = L_0 \oplus K_1$

$L_2 = L_0 \oplus K_1$

$R_2 = R_0 \oplus K_2$

$L_3 = R_0 \oplus K_2$

$R_3 = L_0 \oplus K_1 \oplus K_3$

~~$L_4 = R_0 \oplus K_2$~~

$L_0 \oplus K_1 \oplus R_3 = L_4$

$R_4 = R_0 \oplus K_2 \oplus K_4$ ← response

6d)

$L_i = R_{i-1}$

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

$F(K_{i-1}, K_i) = R_{i-2} \oplus K_i$

L_0, R_0

$L_1 = R_0$

$R_1 = L_0 \oplus R_0 \oplus K_1$

$L_2 = L_0 \oplus R_0 \oplus K_1$

$R_2 = R_0 \oplus L_0 \oplus K_1 \oplus K_2$

$L_3 = R_0 \oplus L_0 \oplus K_1 \oplus K_2$

$R_3 = L_0 \oplus R_0 \oplus K_2 \oplus K_3$

$L_4 = R_0 \oplus K_2 \oplus K_3$

$R_4 = R_0 \oplus L_0 \oplus K_1 \oplus K_3 \oplus K_4$ ← response

8 - a) Ciphertext C:

$C = M^e \mod N$.

$M = 19 \quad d = 7$

$e = 3 \qquad C = 19^3 \mod 33 =$

$N = 33 \qquad 6859 \mod 33 = 28.$

We then do decrypt:

$M = C^d \mod N = 28^7 \mod 33$

$= 19.$

8 - b) In this case: $N = 33$

$M = 25$

$S = M^d \mod N = 25^7 \mod 33 = 31$

Thus $S = 31$.

To verify the signature, Bob will compute $S^e \mod N$. He then compares the obtained value with M (the value received).

In this case we have $S = 31 \quad N = 33$

$31^3 \mod 33 = 25$. We have $M = 25$

thus the signature is verified.

10 a. $\sqrt{2^n} = 2^{n/2}$. From the slides.

b) Such an operation will give about 10×2^n comparisons whereas we expect: $\sqrt{10} \times \sqrt{2^n} = \sqrt{10} \times 2^{n/2}$

c) We can observe from the above question that as we generate more hashes, they gets easier to find a collision. We can compare every new hash with all the previous hashes thus it does get easier.

7 a) $MAC = E(CC_{n-2} \oplus P_{n-1}, k)$

We need to construct the above equation. Since we know k and MAC, we can have $P_{n-1} = D(MAC, k) \oplus C_{n-2}$

Then we can use these values to construct a message with the same MAC.

7 b) All of them except the last one that is the MAC.

9a) If it were that an attacker intercepted the encrypted key $\in(K, X)$, it would be very easy to break free the ~~encryption~~ lines and making it possible to decrypt all ~~the~~ further messages between Alice and Bob.

9b) Instead of exchaging information during the first communication we need to create a key (both sides).

We can have both sides pick a random key K_3 and K_4. We then mix X with K_1 and do the same for K_2. Send the result. We can then, mix the received values with K_1 and K_2 respectively and this may create a secret key over a public network safely, assuming X is only known by Alice and Bob.

9c) It is safer because even if the communication is recorded by an attacker, there is no way for the attacker to figure out what the key is. ~~This assumes~~