Question 1

3 / 3 pts

A person grabs a shirt from a closet in the dark and puts it on. In the closet are two blue shirts, two red shirts, and four yellow shirts. How uncertain is the color of the shirt. Answer in bits of entropy, rounded to the nearest hundredth.

1.5

2 blue shirts Total 8 shirts
2 red
4 yellow

Outcome	Pr	Entropy	Product
Blue	$\frac{2}{8}$	$-\log_2\left(\frac{2}{8}\right) = 2$	$\frac{2}{8} \cdot 2 = \frac{1}{2}$
Red	$\frac{2}{8}$	$-\log_2\left(\frac{2}{8}\right) = 2$	$\frac{2}{8} \cdot 2 = \frac{1}{2}$
Yellow	$\frac{4}{8}$	$-\log_2\left(\frac{4}{8}\right) = 1$	$\frac{4}{8} \cdot 1 = \frac{4}{8}$
			Sum : 1.50

Question 2

4 / 4 pts

In the final key agreement protocol detailed in the textbook, Alice specifies a requested minimum prime p of 3 bits. What are the smallest and largest prime numbers that pass her size test?

See here for a list of primes: https://primes.utm.edu/lists/small/10000.txt

smallest prime: 5

largest prime: 61

Alice's minimum prime p of 3 bits

Given: $s_a = 3$

$s_a - 1 \le \log_2 p \le 2 \cdot s_a$

$3 - 1 \le \log_2 p \le 2 \cdot 3$

$\underset{\text{min}}{2} \le \log_2 p \le \underset{\text{max}}{6}$

min: $2 \le \log_2 p = 4$ must meet 3 bit length and be a prime $\therefore$ 5

max: $\log_2 p \le 6 = 64$ must be a prime and satisfy the RHS condition $\therefore$ 61

Question 3

0 / 4 pts

Consider the final key agreement protocol detailed in the textbook. If Alice and Bob are both honest, and any adversaries are passive, which of the following components could be removed and the resulting protocol would still be well-defined and secure? Check all that apply.

- [ ] s_a
- [ ] N_a
- [ ] (p,q,g)
- [ ] g^x
- [ ] $Auth_B$
- [ ] g^y
- [ ] $Auth_A$

Alice | **Bob**

Alice: $s_a \leftarrow \min p$ size

Alice: $N_a \in_R 0, \ldots, 2^{256} - 1$

Alice → Bob: s_a, N_a

Bob: $s_b \leftarrow \min p$ size

Bob: $s \leftarrow \max(s_a, s_b)$

Bob: $s \overset{?}{\leq} 2 \cdot s_b$

Bob: Choose (p, q, g) with $\log_2 p \geq s - 1$

Bob: $x \in_R \{ 1, \ldots, q-1 \}$

Bob → Alice: (p, q, g), $X := g^x$, $\textsc{Auth}_\textsc{B}$

Alice: Check $\textsc{Auth}_\textsc{B}$

Alice: $s_a - 1 \overset{?}{\leq} \log_2 p \overset{?}{\leq} 2 \cdot s_a$

Alice: $255 \overset{?}{\leq} \log_2 q \overset{?}{\leq} 256$

Alice: Check p, q both prime

Alice: $q \overset{?}{\mid} (p-1) \wedge g \overset{?}{\neq} 1 \wedge g^q \overset{?}{=} 1$

Alice: $X \overset{?}{\neq} 1 \wedge X^q \overset{?}{=} 1$

Alice: $y \in_R \{ 1, \ldots, q-1 \}$

Alice → Bob: $Y := g^y$, $\textsc{Auth}_\textsc{A}$

Bob: Check $\textsc{Auth}_\textsc{A}$

Bob: $Y \overset{?}{\neq} 1 \wedge Y^q \overset{?}{=} 1$

Alice: $k \leftarrow \text{SHA}_d\text{-}256(X^y)$

Bob: $k \leftarrow \text{SHA}_d\text{-}256(Y^x)$

N_a, $Auth_B$, $Auth_A$

Question 4

5 / 5 pts

You saw a simplified version of OCB in lecture. Here's a summary. Let E'(T,X) be a tweakable block cipher that has already been keyed. Given plaintext P = P_1 || P_2 || ... || P_n (ie, P is an n-block plaintext).

C_i = E'(i, P_i) for i=1..n
sum = P_1 xor P_2 xor ... xor P_n
tag = E'(0,sum)

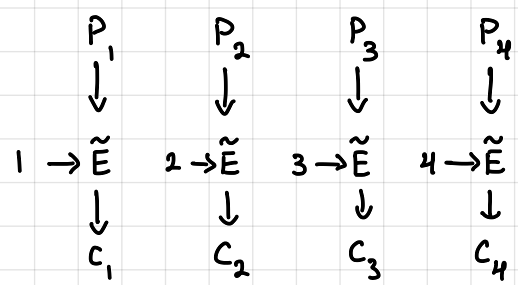
For simplicity let's say that E'(T,X) = ROTL(X,T+1) (ie, X rotated left T+1 bits. If the block cipher block size is 8 bits and you are encrypting the two byte plaintext 81 18 (in hex), what ciphertext and tag would be created? Fill in each box as a two-digit hex value.

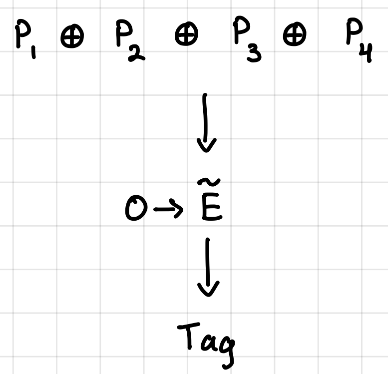
C_1 06

C_2 C0

tag 33

OCB - Authenticated Encryption





C_i are uniform

Advantage = 0

$C_1 = E'(1+1, 81) = 06$

$C_2 = E'(2+1, 18) = C0$

$$\begin{aligned}
Tag &= E'((P_1 \oplus P_2), 0+1) \\
&= E'((81 \oplus 18), 1) \\
&= E'(99, 1) \\
&= 33
\end{aligned}$$

Question 5

1.33 / 4 pts

Consider the Fortuna random generator. Choose the answer that is most correct for each statement.

Forward security is provided by Rekeying the block cipher

Consider the entropy pools P_i and P_{i+1}. In the long run, what is the ratio (number of times P_i is emptied) / (number of times P_{i+1} is emptied)?

[Select]

Consider the entropy pools P_i and P_{i+1}. In the long run, what is the ratio (number of times entropy is added to P_i) / (number of times entropy is added to P_{i+1})?

[Select]

a) Forward security is provided by Reseeding with entropy sources
Backward security is provided by Rekeying the block cipher

b) number of times P_i is emptied is $\frac{1}{2^i}$

reseed_cnt	Pools Emptied
1	P_0
2	P_0 P_1
3	P_0
4	P_0 P_1 P_2
5	P_0
6	P_0 P_1
7	P_0
8	P_0 P_1 P_2 P_3
⋮	

Pool P_i ; used every 2^i reseed

number of times P_{i+1} is emptied is $\frac{1}{2^{i+1}}$

$$\therefore \frac{\frac{1}{2^i}}{\frac{1}{2^{i+1}}} \Rightarrow \frac{1}{2^i} \cdot \frac{2^i + 2^1}{1} \Rightarrow 2$$

c) number of times entropy is added to P_i is $\frac{2^i}{10}$

Reseed after $\frac{1}{10}$ sec

number of times entropy is added to P_i = 1
number of times entropy is added to P_{i+1} = 1

$$\frac{1}{1} = 1$$