CPSC 418 / MATH 318 — Introduction to Cryptography
ASSIGNMENT 1 Problems 1-4

Name: Daniel Heyns **Student ID:** 30021292

Problem 1 — Password length and entropy

(a) Since a bit has two possible values and an ASCII character has 7 bits, the number of possible ASCII characters is 2^7. A password of length 8 would have 8 ASCII characters in a row.

$$2^{7^8} = 2^{56} = 7.21 * 10^{16}$$

(b) (i) Possible printable characters for one character would be

$$\text{uppercase} + \text{lowercase} + \text{numerical digits} + \text{special characters}$$

$$= 26 + 26 + 10 + 32$$

$$= 94$$

we then raise this to a power of 8 as we are looking for an 8 digit password

$$94^8 = 6.10 * 10^{15}$$

(ii) Lower case letters only would reduce the initial options for the character to 26.

$$26^8 = 2.09 * 10^{11}$$

(c) (i) Simple division and multiplication by 100 to find the percentage.

$$\text{Any Printable Characters/Total} * 100$$

$$= 94^8/2^{56} * 100 = 8.46\%$$

(ii) Simple division and multiplication by 100 to find the percentage.

$$\text{Lower Case/Total} * 100$$

$$= 26^8/2^{56} * 100 = 0.00028\%$$

(d) (i) Entropy of equally likely outcomes

$$H(x) = log_2(n)$$

where $n \in \mathbb{N}$ is the number of possible inputs.

$$H(x) = log_2(94^8) = 52.45$$

(ii)

$$H(x) = log_2(26^8) = 37.60$$

(e) (i) Let z be the length of the password.

$$H(x) = log_2(94^z) = 128$$
$$2^{128} = 94^z$$
$$z = \frac{128log(2)}{log(94)} = 19.528$$

Round up to 20 as this is password length.

(ii) Let z be the length of the password.

$$H(x) = log_2(26^z) = 128$$
$$2^{128} = 26^z$$
$$z = \frac{128log(2)}{log(26)} = 27.23$$

Round up to 28 as this is password length.

Problem 2 — One-time pad without the all-zeros key

(a) $p(M) = p(M|C)$ for all plaintexts M and ciphertexts C with $p(C) > 0$, is the definition of perfect secrecy. We will use the negated form to prove the opposite when the zero pad is removed.
The negation would be: There exists a plaintext M and ciphertext C with $p(C) > 0$ where $p(M) \neq p(M|C)$.

Let $n = 1$ that is $M \in \{0,1\}, C \in \{0,1\}$ and $K \in \{1\}$ as we remove $K = 0^n = 0^1 = 0$. Let $i \in \mathbb{N}$ be the number of possibilities for M and C, in this case 2.

$$K \in \{1\} \text{ therefore } K = 1$$

$$P(M) = \frac{1}{i}$$
$$P(M) = 0.5$$

$$\begin{aligned} D_K(C) &= C \oplus K \\ &= C \oplus 1 \\ &= \bar{C} = M \text{ (Where } \bar{C} \text{ is the inverse of C)} \end{aligned}$$

Because $\bar{C} = M$ in this case, we know M given C.
$P(M|C) = 1 \neq 0.5 = P(M)$

(b) Even if a bit string is not hidden, an attacker has no way of knowing whether the cipher has been encrypted or not. The one-time pad could encrypt plain-text into any cipher, including other sensible statements. In fact the likely hood of a plain-text being encrypted to another sensible output with the one-time pad is much higher than the $K = 0^n$ possibility on average.

Problem 3 — Weak collisions

(a) Since n is the number of possible assigned numbers, the probabilitiy of assigning a specific value N to a participant is $\frac{1}{n}$

(b) 1 is the total probability, therefore the probability of not being assigned a specific number is $1 - \frac{1}{n}$

(c) We put the probability of one person not being assigned N to the power of the given number of people k, as we are calculating the probability of an event occurring multiple times in a row. $(1 - \frac{1}{n})^k$

(d) 50% collision means 50% probability of no collision, we can use the above formula with a less than or equal to 0.5 probability, using $n = 10$.

$$
\begin{aligned}
(1 - \frac{1}{10})^k &\leq 0.5 \\
log(0.9^k) &\leq log(0.5) \\
k &\geq \frac{log(0.5)}{log(0.9)}, \text{ (flip inequality, log(0.9) is negative)} \\
k &\geq 6.58
\end{aligned}
$$

Round up as we are calculating the minimum number of people to ensure the chance of a weak collision is above 50%. Final answer is 7.

(e)

Starting with equation (1)

$$1 - x < e^{-x}$$

We replace x with $\frac{1}{n}$ and raise both sides of the equation to $log(2)n$

$$
\begin{aligned}
(1 - \frac{1}{n})^{log(2)n} &< (e)^{\left(-\frac{1}{n}\right)^{log(2)n}} \\
(1 - \frac{1}{n})^{log(2)n} &< (e)^{-log(2)} \\
(1 - \frac{1}{n})^{log(2)n} &< 0.5 \\
1 - (1 - \frac{1}{n})^{log(2)n} &> 0.5 \text{ (multiply each side by -1 and add 1)}
\end{aligned}
$$

$1 - (1 - \frac{1}{n})^k$ is the expression for the probability of a weak collision occurring. We see that when $k = log(2)n$ the probability is above 0.5 and if k were to grow the left side would grow as well. Therefore if $k \geq log(2)n$ the probability of a weak collision occurring with be equal to or greater than 50%

Problem 4 — (Strong) collisions

(a) The probability of choosing a number someone else has already chosen increases the more people who have gone before you. We can start with the probability of an individual colliding.

$$\frac{i-1}{n}$$

where i is the number of people who have gone before you and n is size of the pool of numbers. We invert this to find the probability of no collision and then we must multiply all participants' probabilities together to find the probability of no collisions.

$$\prod_{i=1}^{k}\left(1-\frac{i-1}{n}\right)$$

(b) The probability of a collision occuring is the inverse of no collision occurring.

$$1-\prod_{i=1}^{k}\left(1-\frac{i-1}{n}\right)$$

(c) We will use a table to solve this problem. Let n = 10. The Result table is the outcome of the above equation with k set to the designated value.

k	Result
1	0
2	0.1
3	0.28
4	0.496
5	0.6976

We see that between 4 participants and 5 we reach a probability of 0.5 for collision. We need at least 5 participants to ensure a 50% chance of collision.

(d) For this proof I will use the closed-form expression for the nth triangular number.

$$\sum_{i=1}^{t}=\frac{t(t+1)}{2} \tag{2}$$

Starting with equation(1).

$$1 - x < e^{-x}$$

$$\prod_{i=1}^{k}\left(1 - \frac{i-1}{n}\right) < \prod_{i=1}^{k}\left(e^{-\frac{i-1}{n}}\right) \text{ (replace x with } \frac{i-1}{n} \text{ and apply the product operator)}$$

$$= e^{-\frac{1-1}{n}} * e^{-\frac{2-1}{n}} \ \ldots \ * e^{-\frac{k-1}{n}}$$

$$= e^{-(\frac{0}{n}+\frac{0}{n} \ \ldots \ +\frac{k-1}{n})}$$

$$= e^{-\sum_{i=1}^{k-1}\frac{i}{n}}$$

$$= e^{-\sum_{i=1}^{k-1} i\frac{1}{n}}$$

$$= e^{-\left(\frac{k(k-1)}{2}\right)\frac{1}{n}} \text{ (use equation (2))}$$

$$= e^{-\left(\frac{k(k-1)}{2n}\right)}$$

End of proof.

(e) We start with the following equation given.

$$P = e^{\frac{-k^2}{2n}}$$

Replacing k with $\sqrt{log(4)n}$ we get the following.

$$P = e^{\frac{-\left(\sqrt{log(4)n}^2\right)}{2n}}$$

$$P = e^{\frac{-log(4)n}{2n}}$$

$$P = e^{\frac{-log(4)}{2}}$$

$$P = \frac{1}{2}$$

We see that when $k = \sqrt{log(4)n}$ the probability of no collision is equal to 0.5. We can assume that should k in the formula $P = e^{\frac{-k^2}{2n}}$ increase, P shall decrease. Therefore should $k \geq \sqrt{log(4)n}$, $P \leq 0.5$ and the inverse probability that there will be a collision, $P_c \geq 0.5$.