2.1 Basics on libraries

2.1.1 Probabilities

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

- **Pr$[A_1 \diamond L_1 \Rightarrow 1]$:**

  $\Pr[(r_1 \leftarrow \mathbb{Z}_6) \stackrel{?}{=} (r_2 \leftarrow \mathbb{Z}_6)] = \frac{1}{6}$
- **Pr$[A_1 \diamond L_2 \Rightarrow 1]$:**

  $\Pr[0 \stackrel{?}{=} 0] = 1$
- **Pr$[A_2 \diamond L_1 \Rightarrow 1]$:**

  $\Pr[(r \leftarrow \mathbb{Z}_6) \stackrel{?}{\geq} 3] = \frac{1}{2}$
- **Pr$[A_2 \diamond L_2 \Rightarrow 1]$:**

  $\Pr[0 \stackrel{?}{\geq} 3] = 0$

2.1.2 Equivalent libraries

Two Libraries L_{left} and L_{right} are equivalent iff:

$$P[A \diamond L_{left} \rightarrow 1] = P[A \diamond L_{right} \rightarrow 1]$$

L_{left}		L_{right}
QUERY():	$\stackrel{?}{\equiv}$	QUERY():
x $\leftarrow \{0,1\}^n$		x $\leftarrow \{0,1\}^n$
return x		y := $\overline{x}$
		return y

  Because we can make a 1:1 correspondence (we could make a bijection) for each return value of L_{left} to each return value of L_{right} the probabilities for each return value are equal and therefore the libraries are equivalent.

L_{left}		L_{right}
QUERY():	$\stackrel{?}{\equiv}$	QUERY():
x $\leftarrow \mathbb{Z}_n$		x $\leftarrow \mathbb{Z}_n$
return x		y := 2x % n
		return y

  For "even" n's:
  Let us assume that n = 2 and we calculate the probability of the return value being 1. In this case $\mathbb{Z}_2 = \{0, 1\}$ and the probability of L_{left} returning 1 is therefore $\frac{1}{2}$. The library L_{right} will only return 1 if there is a possibility to solve the equation 1 = 2x % 2, with x $\in \mathbb{Z}_2$. Because there is no possible result L_{right} cannot return 1, so the probability is 0 and the libraries are therfore not equivalent.

For "uneven" n's:
For uneven n, the distributions are:

$$\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$$

$$2 \cdot \mathbb{Z}_n \% n = \{0, 2, 4, ..., n-1, 1, 3, ..., n-2\}$$

Therefore the second distribution is a permutation of the first one and therefore the libraries are equivalent.

-

L_{left}		L_{right}
QUERY():	$\stackrel{?}{\equiv}$	QUERY():
x $\leftarrow \{0,1\}^n$		z $\leftarrow \{0,1\}^n$
y $\leftarrow \{0,1\}^n$		return z
return x & y		

  Let us assume that n = 1. The probability of L_{left} returning 0 is $\frac{3}{4}$ because this is returned if $((x = 0) \wedge (y = 0)) \vee ((x = 0) \wedge (y = 1)) \vee ((x = 1) \wedge (y = 0))$. Only if $((x = 1) \wedge (y = 1))$ L_{left} returns 1. L_{right} will return 0 with a possibility of $\frac{1}{2}$. Therefore they are not equivalent.

2.2 Security of a modified One-time Pad (OTP)

7 Given the two libraries from the lecture, we need to show that $L_{OTS_left} \equiv L_{OTS_right}$ so we can conclude the one-time secrecy:
For two arbitrary messages m_1 and m_2, the eavesdrop() function will return the following bit string for either of the two libraries:

$$c_1 c_2 \cdots c_{n-2} c_{n-1} c_n$$

whereas: $c_{n-1} = c_n = 0$ *and* $c_1, c_2, \cdots, c_{n-2}$ *are uniformaly distributed in* $\{0, 1\}^{n-2}$

Because in either cases the ciphertexts will be distributed in the same way, a distinguishable algorithm A still will be unable to differ between those two libraries. This implies that both libraries are exchangeable due to the fact that $P[A \diamond L_{OTS-left} \Rightarrow 1] = P[A \diamond L_{OTS-right} \Rightarrow 1]$. So this cipher will provide a one time secrecy. $\square$

2.3 Construction of a distinguisher

First we can make a few assumptions:

1. If at least one of m OR k is even the result for $(k \times m)\%10$ is even
2. Only if m and k are odd the result for $(k \times m)\%10$ is odd

Therefore we can compute the following table:

	k even	k odd
m even	c even	c even
m odd	c even	c odd

Now we can define a distinguishing algorithm A:

$$
\begin{aligned}
&A:\\
&\quad m_l \leftarrow 2\\
&\quad m_r \leftarrow 3\\
&\quad c = Eavesdrop(m_l, m_r)\\
&\quad if\ (c\ mod\ 2\ ==\ 0)\ \{\\
&\qquad \frac{2}{3}\ likelihood\ that\ m_l\ encrypted\\
&\qquad return\ 0\\
&\quad \}\\
&\quad else\ \{\\
&\qquad Guaranteed\ that\ m_r\ is\ encrypted\\
&\qquad return\ 1\\
&\quad \}\\
&\quad end
\end{aligned}
$$

Therefore for the probability follows:

$$P[A \diamond L_{OTS-left} \Rightarrow 1] = 0 \neq \frac{1}{2} = P[A \diamond L_{OTS-right} \Rightarrow 1]$$

We can see that this leads to the conclusion that the two libraries are NOT exchangeable and therefore the one-time secrecy cannot be provided.

2.4* Size of the OTP key space

-