Cryptographic protocols
Exercise 2

Ilja Kuzovkin

December 30, 2010

1 Evaluate a Yao's circuit

1.1 Functionality

After some trials I came to conclusion that this circuit's function is multiplication of two binary numbers $\overline{x_1 x_0}$ and $\overline{y_1 y_0}$

```
00 * 00 = 0000
00 * 10 = 0000
00 * 01 = 0000
00 * 11 = 0000
10 * 00 = 0000
10 * 10 = 0100
10 * 01 = 0010
10 * 11 = 0110
01 * 00 = 0000
01 * 10 = 0010
01 * 01 = 0001
01 * 11 = 0011
11 * 00 = 0000
11 * 10 = 0110
11 * 01 = 0011
11 * 11 = 1001
```

1.2 Evaluation

First we can evaluate $out0$ and deduce x_0 and y_0. We compute $E(K0, E(K2, K5_0))$ and $E(K0, E(K2, K5_1))$ and see if which of possible ciphertexts

```
E(K0_0,E(K2_0,K5_0)) = 82A24FE22DF65C4DC22E0122E4587EF3
E(K0_0,E(K2_1,K5_0)) = 96726747E168BF48BE5821787B40D184
E(K0_1,E(K2_0,K5_0)) = 14C7E5632F71A7618302337D73D82A3C
E(K0_1,E(K2_1,K5_1)) = 3E0CD86B5D2C07DA9AA5E6FCDF7D2BF4
```

we will get.

```
E(K0_?, E(K2_?, K5_0)) = E(00000000D9D50296847914E61429742E,
  E(0000000021838E099FB657A0E517B495, 00000000434E23A0273904BEA0E2DCF6)) =
  = E(00000000D9D50296847914E61429742E, 228797567EA70EB7ADEB78C4F34D489D) =
  = 8BA7A50A65FFF8B708A6311D4D7EA33F
E(K0_?, E(K2_?, K5_0)) = E(00000000D9D50296847914E61429742E,
  E(0000000021838E099FB657A0E517B495, 000000006C1E5EDEF8A84DE31F4DF7E4)) =
  = E(00000000D9D50296847914E61429742E, CB16490FB707D200B9F10A5BDACA5F17) =
  = 3E0CD86B5D2C07DA9AA5E6FCDF7D2BF4
```

As we can see second attempt gave us one of ciphertexts expected, now we know that keys $K0\_1$ and $K2\_1$ were used, which means $x_0 = 1$ and $y_0 = 1$.
Next node to deduce is K4. We have 4 ciphertexts, keys $K3\_?$ and $K0_1$, and we know that decryption of correct cipher should give a key $K4\_?$ starting with 00000000.

```
D(K3_?, D(K0_1, K4)) = D(00000000953DFE728999DB98ABACE339,
  D(00000000D9D50296847914E61429742E, 83EC2D6387FD44A26BFB1F1C44966412) =
  = e0acd37f6a70665cf45a813f337dfb8f
D(K3_?, D(K0_1, K4)) = D(00000000953DFE728999DB98ABACE339,
  D(00000000D9D50296847914E61429742E, 383B630696784899B426B0E17632F19C) =
  = c315f7f333ad90662ab2d33cdc46989d
D(K3_?, D(K0_1, K4)) = D(00000000953DFE728999DB98ABACE339,
  D(00000000D9D50296847914E61429742E, B9980777A18C32D89C0FE7B2D9336F60) =
  = beff2ff30eeb224b735b9de3739fe07d
D(K3_?, D(K0_1, K4)) = D(00000000953DFE728999DB98ABACE339,
  D(00000000D9D50296847914E61429742E, 0ED40C522DBCF05C5D4FFF23853F6FCA) =
  = 00000000e795130d3a3f2f4a020059d7
```

Now we know that K4_? key is 00000000e795130d3a3f2f4a020059d7. At this point we don't yet know value of K4 and y1.
We will do same operation for all internal nodes.

K6

```
D(K3_?, D(K1_?, K6)) = D(00000000953DFE728999DB98ABACE339,
  D(00000000B12876E4B37DAA4CE9ADFAE2, 58C25210718C4F6F03559B775DBF7836) =
  = fd7055abbe413de6947971bec36c54ef
D(K3_?, D(K1_?, K6)) = D(00000000953DFE728999DB98ABACE339,
  D(00000000B12876E4B37DAA4CE9ADFAE2, 5101622E6D522ADDA6D805A9268F8009) =
  = 21d4621d2ca4d4515b454f7c5db1c898
D(K3_?, D(K1_?, K6)) = D(00000000953DFE728999DB98ABACE339,
  D(00000000B12876E4B37DAA4CE9ADFAE2, 6EF37D17EA7F62C008B677D9B8BD93E5) =
  = 8abeeb0c4e87ed6c3bfeefe1344280ff
D(K3_?, D(K1_?, K6)) = D(00000000953DFE728999DB98ABACE339,
  D(00000000B12876E4B37DAA4CE9ADFAE2, 769044959D7C7E5E470EF0C1655C26C2) =
  = 00000000acdedd61c4c002f7bcb294cd
```

Key K6_? is 00000000acdedd61c4c002f7bcb294cd

K7

```
D(K2_1, D(K1_?, K7)) = D(0000000021838E099FB657A0E517B495,
  D(00000000B12876E4B37DAA4CE9ADFAE2, 6BCF4FBA28EC730BC56F989CD52DDD13) =
  = ...
D(K2_1, D(K1_?, K7)) = D(0000000021838E099FB657A0E517B495,
  D(00000000B12876E4B37DAA4CE9ADFAE2, A560F474E3E1D4027665789F142D3F49) =
  = ...
D(K2_1, D(K1_?, K7)) = D(0000000021838E099FB657A0E517B495,
  D(00000000B12876E4B37DAA4CE9ADFAE2, 3686FA7E5A3BFFE6194CA5A4647398CE) =
  = ...
D(K2_1, D(K1_?, K7)) = D(0000000021838E099FB657A0E517B495,
  D(00000000B12876E4B37DAA4CE9ADFAE2, 495E2D566E9992C6DB4FC1D59D07DC67) =
  = 00000000b712347fa17d33ed304e7f40
```

Key K7_? is 00000000b712347fa17d33ed304e7f40

K8

```
D(K7_?, D(K4_?, K8)) = D(00000000b712347fa17d33ed304e7f40,
  D(00000000e795130d3a3f2f4a020059d7, CDA95962028469A59AD9C2B01D7BCC85) =
  = ...
D(K7_?, D(K4_?, K8)) = D(00000000b712347fa17d33ed304e7f40,
  D(00000000e795130d3a3f2f4a020059d7, 97480CAECD3D45F54A073D373922CCDD) =
  = ...
D(K7_?, D(K4_?, K8)) = D(00000000b712347fa17d33ed304e7f40,
  D(00000000e795130d3a3f2f4a020059d7, 396C7B45953C55E66C23786E153BEC2D) =
  = ...
D(K7_?, D(K4_?, K8)) = D(00000000b712347fa17d33ed304e7f40,
  D(00000000e795130d3a3f2f4a020059d7, 1B630F12E535CB7F984941CDD00BB382) =
  = 0000000091298a764c2fb1ef352c9d83
```

Key K8_? is 0000000091298a764c2fb1ef352c9d83

K9

```
D(K7_?, D(K4_?, K9)) = D(00000000b712347fa17d33ed304e7f40,
  D(00000000e795130d3a3f2f4a020059d7, 0DFA5293092BA584E9482C9DF3041497) =
  = ...
D(K7_?, D(K4_?, K9)) = D(00000000b712347fa17d33ed304e7f40,
  D(00000000e795130d3a3f2f4a020059d7, 5DF26939D57A4B86895D585FBB30575B) =
  = ...
D(K7_?, D(K4_?, K9)) = D(00000000b712347fa17d33ed304e7f40,
  D(00000000e795130d3a3f2f4a020059d7, 7474C47E576052FC6B67B67777CD3B8E) =
  = ...
D(K7_?, D(K4_?, K9)) = D(00000000b712347fa17d33ed304e7f40,
  D(00000000e795130d3a3f2f4a020059d7, 6AD1AE4E990975F641A5A9551B31C2C3) =
  = 00000000ecbceb199c2099cd7275652f
```

Key K9_? is 00000000ecbceb199c2099cd7275652f
In fact we know also that:
K9 that indicate 0: 00000000 19EBBCEC CD99209C 2F657572
K9 that indicate 1: 00000000 736BDE7F 8EE29E65 0836EE03
So now we can tell, that K9 = 0
Key K9_0 is 00000000ecbceb199c2099cd7275652f

K10

```
D(K8_?, D(K6_?, K10)) = D(0000000091298a764c2fb1ef352c9d83,
  D(00000000acdedd61c4c002f7bcb294cd, 6CBA66EBEB94935A89FBC99CB9E1BBA6) =
  = ...
D(K8_?, D(K6_?, K10)) = D(0000000091298a764c2fb1ef352c9d83,
  D(00000000acdedd61c4c002f7bcb294cd, 19C7A04D07FD6237C0217CA8A4D5BF45) =
  = ...
D(K8_?, D(K6_?, K10)) = D(0000000091298a764c2fb1ef352c9d83,
  D(00000000acdedd61c4c002f7bcb294cd, FE2781784B2AF5C8C532DA414E4DBE43) =
```

```
  = ...
D(K8_?, D(K6_?, K10)) = D(0000000091298a764c2fb1ef352c9d83,
  D(00000000acdedd61c4c002f7bcb294cd, BA69E77DE0FD06DFB6DFAA59B12CC196) =
  = 00000000964e0d0df1dfa097049dbc3a
```

Key K10_? is 00000000964e0d0df1dfa097049dbc3a
Which means K10 = 1
Key K10_1 is 00000000964e0d0df1dfa097049dbc3a

K11

```
D(K8_?, D(K6_?, K11)) = D(0000000091298a764c2fb1ef352c9d83,
  D(00000000acdedd61c4c002f7bcb294cd, 2C46FF26A06F6AAAA4CA5D3F0279531D) =
  = ...
D(K8_?, D(K6_?, K11)) = D(0000000091298a764c2fb1ef352c9d83,
  D(00000000acdedd61c4c002f7bcb294cd, BF3F4B08B462869FA4B1ACB68CA98EC9) =
  = ...
D(K8_?, D(K6_?, K11)) = D(0000000091298a764c2fb1ef352c9d83,
  D(00000000acdedd61c4c002f7bcb294cd, 2F6654C61F193D6A3ADA00606CF5058C) =
  = ...
D(K8_?, D(K6_?, K11)) = D(0000000091298a764c2fb1ef352c9d83,
  D(00000000acdedd61c4c002f7bcb294cd, 876B3AD6E49967CC1CA4144703E1E0AE) =
  = 00000000fb519fe77db8ff5c8fcda936
```

Key K11_? is 00000000fb519fe77db8ff5c8fcda936
Which means K11 = 0
Key K11_0 is 00000000964e0d0df1dfa097049dbc3a

Now we know all output values, which are $out3 = K10 = 1, out2 = K11 = 0, out1 = K9 = 0, out0 = K5 = 1$. So the final output of $f(x1, x0, y1, y0) = 1001$

```
11 * 11 = 1001
```