15. Udowodnić, że dla n=2, $H(X)$ jest to maksymalna dla p_1=p_2=1/2.

$$-\left(\frac{1}{2}\log_2\left(\frac{1}{2}\right)+\frac{1}{2}\log_2\left(\frac{1}{2}\right)\right)=1$$

Ogólniej każde źródło dające **N** równie prawdopodobnych wyników ma $\log_2 N$ bitów na symbol entropii:

$$-\sum_{i=1}^{N}\frac{1}{N}\log_2\frac{1}{N}=-N\frac{1}{N}\log_2\frac{1}{N}=-\log_2\frac{1}{N}=\log_2 N$$

U nas N = 2 więć $\log_2 2 = 1$

16. Jakie są największe wspólne dzielniki dla (95, 47) = ?, i (42, 88) = ? (*Algorytm Euklidesa*).

SPOSÓB 1
(95,47) 95 – 47 = 48
(48,47) 48 – 47 = 1
(47,1) 47 – 1 = 46
...
(2,1) 2 – 1 = 1
NWD = 1

(88,42) 88 – 42 = 46
(46,42) 46 – 42 = 4
(42,4) 42 – 4 = 38
...
(6,4) 6 – 4 = 2
(4,2) 4 – 2 = 2
NWD = 2

SPOSÓB 2
KROK I 95 mod 47 = 1
KROK II 47 mod 1 = 0
WYNIK: 1

KROK I 88 mod 42 = 4
KROK II 42 mod 4 = 2
KROK III 4 mod 2 = 0
WYNIK: 2

17. Jakie są największe wspólne dzielniki dla (99, 87)=?, i (22, 28)=? (*Binary Algorithm*).

99 | **3**
33 | 3
11 | 11
1 |

87 | **3**
29 | 29
1 |

NWD(99,87) = 3

28 | **2**
14 | 2
7 | 7
1 |

22 | **2**
11 | 11
1 |

NWD(28,22) = 2

18. Oblicz wartość *ψ(n)* dla *n*=20, *n*=88, *n*=79.

https://en.wikipedia.org/wiki/Euler%27s_totient_function

$$\varphi(p) = p - 1.$$

$$\varphi(mn) = \varphi(m)\varphi(n).$$

$$\varphi(p^k) = p^{k-1} * (p - 1).$$

ψ(20) = ψ(5∗2∗2) = ψ(5) ∗ ψ(2^2) = 4 ∗ 2 ∗ 1 = 8
ψ(88) = ψ(11∗2∗2∗2) = ψ(11) ∗ ψ(2^3) = 10 ∗ 4 ∗ 1 = 40
ψ(79) = 78

19. Pokaż, że 25^8=1 *mod* 17.

25 mod 17 = 8
$8^8 = 64^4$
64 mod 17 = 13
$13^4 = 169^2$
169 mod 17 = 16
16^2 = 256
256 mod 17 = 1

20. Dla każdego równania postaci *ax=b mod n* przedstawionogo poniżej, uzyskać rozwiązania dla *x* w przedziale [0, *n*–1].

5*x*=2 *mod* 17;

5x = 2 | *4
20x = 8 mod 17 => 3x = 8
3x = 8 | *6
18x = 48 mod 17 => x = 14

19*x*=7 *mod* 26;

19x = 7 | *2
38x = 14 mod 26 => 12x = 14
12x = 14 | * 3
36x = 42 mod 26 => 10x = 16
10x = 16 | * 3
30x = 48 mod 26 => 4x = 22

4x = 22 | * 7
28x = 154 mod 26 => 2x = 24
2x = 24 | * 13
26x = 312 mod 26 => x = 0
13*x*=21 *mod* 26;

13x = 21 | *2
26x = 42 mod 26 => 0x = 16 , brak rozwiazan

25*x*=10 *mod* 100.

25x = 10 | *4
100x = 40 mod 100 => 0x = 40 , brak rozwiazan

21. Udowodnić, że K=E0E0E0E0F1F1F1F1, i K=1F011F010E010E01, jest polu słaby (semiweak) klucze do DES.

????

22. Należy podać odpowiedzi na poniższe przykłady dla IDEA algorytmu:

W przypadku, gdy występują same 0 to negujemy to na 1

0000×0000 *mod* (2^4+1)=?
1111x1111 mod 17 => 15x15 mod 17 => 225 mod 17 => 4

00000000×00001111 *mod* (2^8+1)=?
11111111x00001111 mod 257 => 255x15 mod 257 => 3825 mod 257 => 227

1100+1000 *mod* (2^4)=?
12+8 mod 16 => 20 mod 16 => 4

11100000+01111111 *mod* (2^8)=?
224+127 mod 256 = 95

1100⊕1000=?
0100 = 4

11100000⊕01111111=?
10011111 = 159