1. Compute 45-1(mod 547) by using the extended Euclidean algorithm. [10 points]

> $$\begin{aligned} 45^{-1} &\pmod{547} \\ 547 &= 45(12) + 7 \\ 45 &= 7(6) + 3 \\ 7 &= 3(2) + 1 \end{aligned} \tag{1}$$
>
> So we have:
>
> $$547 + 45(-12) = 7 \tag{2}$$
>
> $$45 + 7(-6) = 3 \tag{3}$$
>
> $$7 + 3(-2) = 1 \tag{4}$$
>
> From (3) and (4), we have:
>
> $$\begin{aligned} 7 + [45 + 7(-6)](-2) = 1 \\ 7(13) + 45(-2) = 1 \end{aligned} \tag{5}$$
>
> From (2) and (5), we have:
>
> $$\begin{aligned} [547 + 45(-12)](13) + 45(-2) = 1 \\ 547(13) + 45(-158) = 1 \pmod{547} \end{aligned} \tag{6}$$
>
> Then
>
> $$\begin{aligned} 45(-158) = 1 \pmod{547} \\ 45(547 - 158) = 1 \pmod{547} \\ 45(389) = 1 \pmod{547} \end{aligned} \tag{7}$$
>
> Hence, the result is 389

2. Compute 5^12242(mod 13) by using the Euler theorem. [10 points]

> $\phi(13) = 12$, so $5^{12} = 1 \bmod 13$
>
> $5^{12242} \equiv (5^{12})^{1020} * 5^2 \equiv 5^2 = 12 \bmod 13$

3. The ciphertext "ZFVALYO" was encrypted by an Affine cipher. The first two letters of the plaintext are "co". Decrypt it. [15 points]

> We know 2 maps to 25, and 14 maps to 5. Assume the function is $y = ax + b$.
>
> $$\begin{aligned} 25 = 2x + b \bmod 26 \\ 5 = 14x + b \bmod 26 \end{aligned} \tag{8}$$
>
> Then We have $12x = -20 = 6 \bmod 26$. Since $gcd(12, 26) = 2$, then we have two solutions $a = 7, 20$. The corresponding values of b are both 11. Now we have two candidates for keys $(7, 11), (20, 11)$.
>
> However, $gcd(20, 26) \neq 1$, we rule out the key $(20, 11)$. Hence, the solution is a = 7, b = 11.

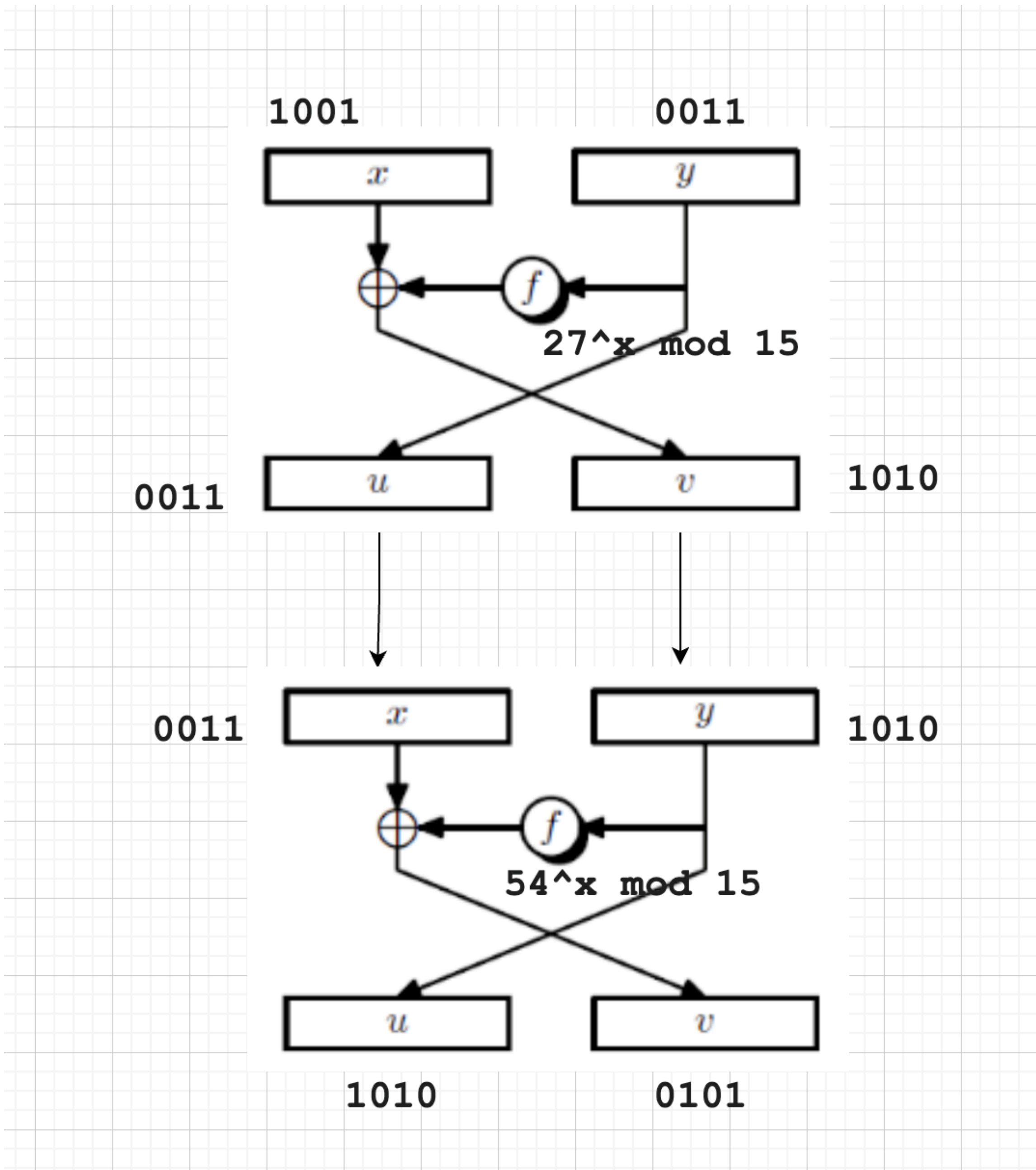
4. Perform El-Gamal encryption for the following setting and compute what Bob will output. [20 points]

P: 8429
G: 3486
M: 156
Alice's random number a: 84
Bob's random number b: 124
H(x, y): 8-LSB of x XOR y
Es(k, m): k XOR m
LSB: Least Significant Bit(s)

> $sk = \alpha = 84$
>
> $u = g^{\alpha} = 3486^{84} \bmod 8429 = 2697$
>
> $v = g^{\beta} = 3486^{124} \bmod 8429 = 5953$
>
> $w = u^{\beta} = 2697^{124} \bmod 8429 = 264$
>
> $k = H(v, w) = 01001001$
>
> $c = E_s(k, m) = 01001001 \text{ XOR } 10011100 = 11010101 = 213$

5. Consider a block cipher using 8-bit blocks that is based on the basic DES architecture (Feistel network) with two rounds and no initial or final permutation. The scrambling function for round *i* is fi (x, k) = (3i * k)x mod 15, for i = 1, 2, where the key k is a member of Z15. If K = 9 and the ciphertext is 10100101, what is the plaintext?[15 points] Draw the Feistel cipher network for the two rounds. [10 points]

> We know the round function is $f_i(x, k) = (3i * k)^x \bmod 15$.
>
> In the first round, we have $f_1(x, 9) = 27^x \bmod 15$.
>
> In the second round, we have $f_2(x, 9) = 54^x \bmod 15$.
>
> By the Feistel permutation, we have $\pi(x, y) := (y, x \oplus f(y))$, so
> $\pi_2(x_2, y_2) := (y_2, x_2 \oplus f_2(y_2)) = 10100101$, where $y_2 = u_2 = 1010, x_2 \oplus f_2(y_2) = v_2 = 0101$
>
> The inverse will be
> $\pi_2^{-1}(u_2, v_2) = (v_2 \oplus f_2(u_2), u_2) = (0101 \oplus f_2(1010), 1010) = (0101 \oplus 0110, 1010) = (0011, 1010)$
>
> Now we get $\pi_1(x_1, y_1) = (0011, 1010) = (u_1, v_1)$ and $\pi_1^{-1}(u_1, v_1) = (v_1 \oplus f_1(u_1), u_1)$,
>
> then $(x_1, y_1) = \pi_1^{-1}(u_1, v_1) = (v_1 \oplus f_1(u_1), u_1) = (1010 \oplus 0011, 0011) = (1001, 0011)$
>
> Hence the plaintext is 10010011 and the Feistel cipher network is as follows:


1001
0011
x
y
f
27^x mod 15
0011
u
v
1010
0011
x
y
1010
f
54^x mod 15
u
v
1010
0101