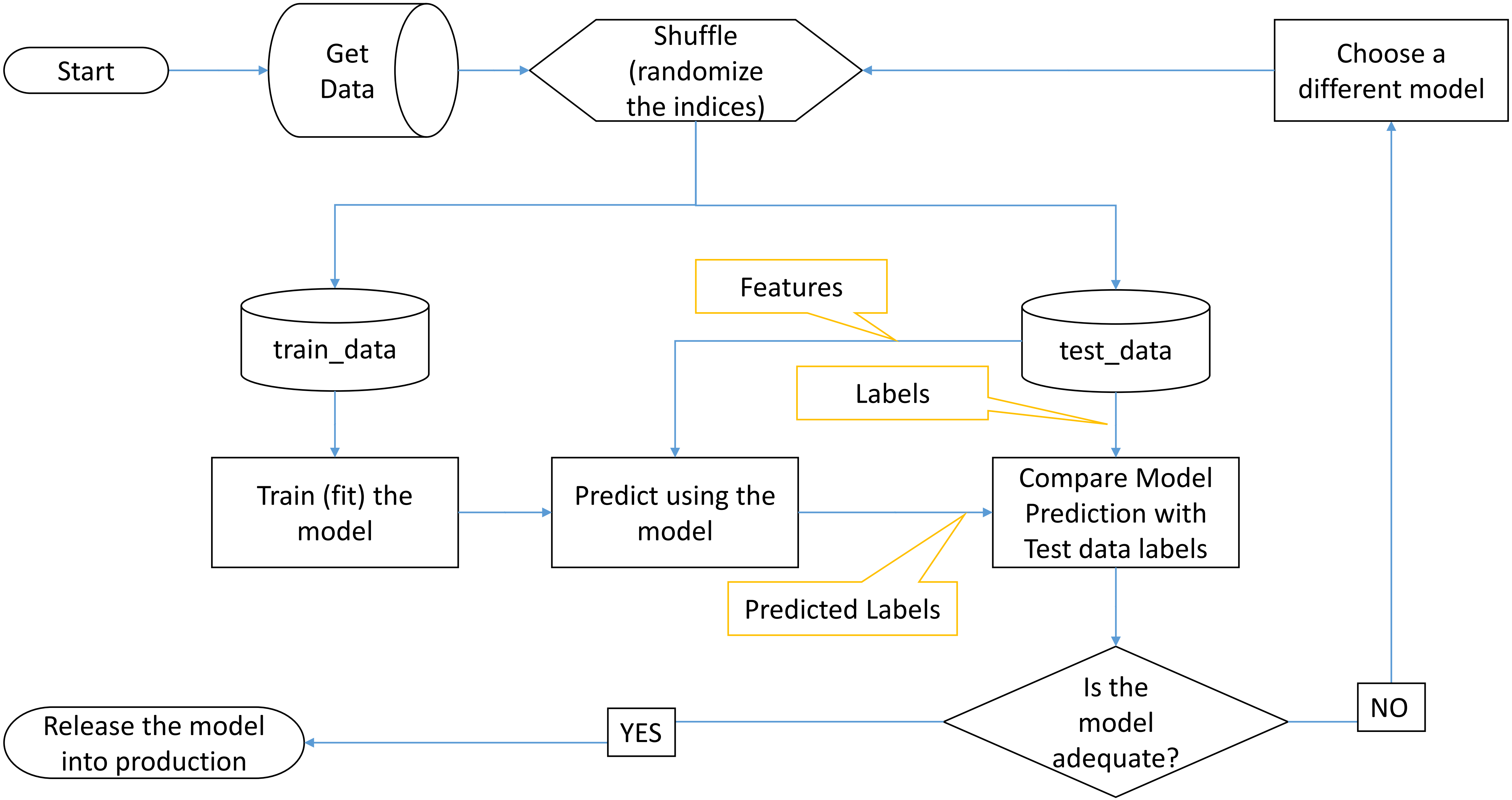
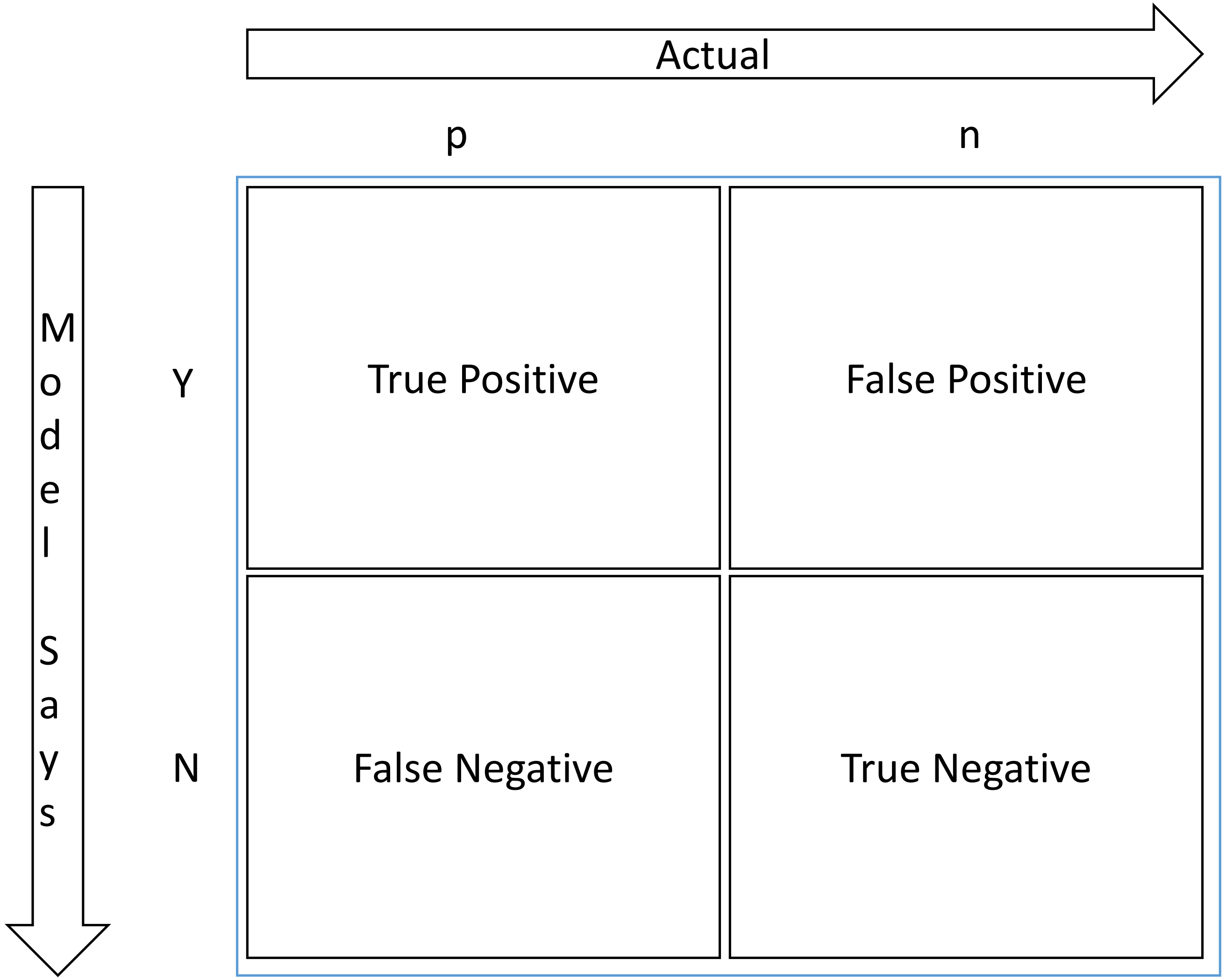

Start
Get Data
Shuffle (randomize the indices)
Choose a different model
train_data
Features
test_data
Labels
Train (fit) the model
Predict using the model
Compare Model Prediction with Test data labels
Predicted Labels
Is the model adequate?
NO
YES
Release the model into production

Binary Confusion Matrix

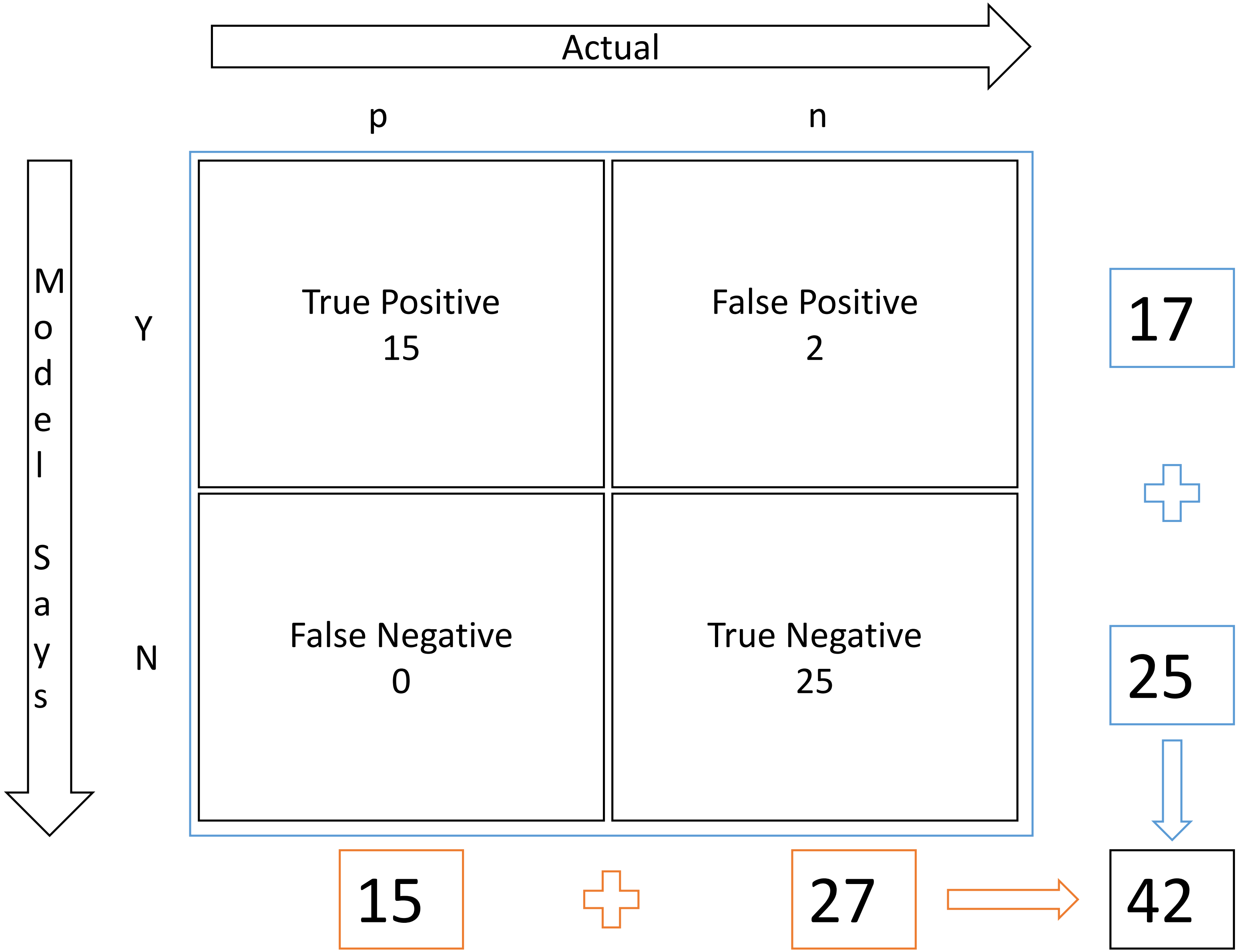


Actual

Model Says

	p	n
Y	True Positive	False Positive
N	False Negative	True Negative

Binary Confusion Matrix

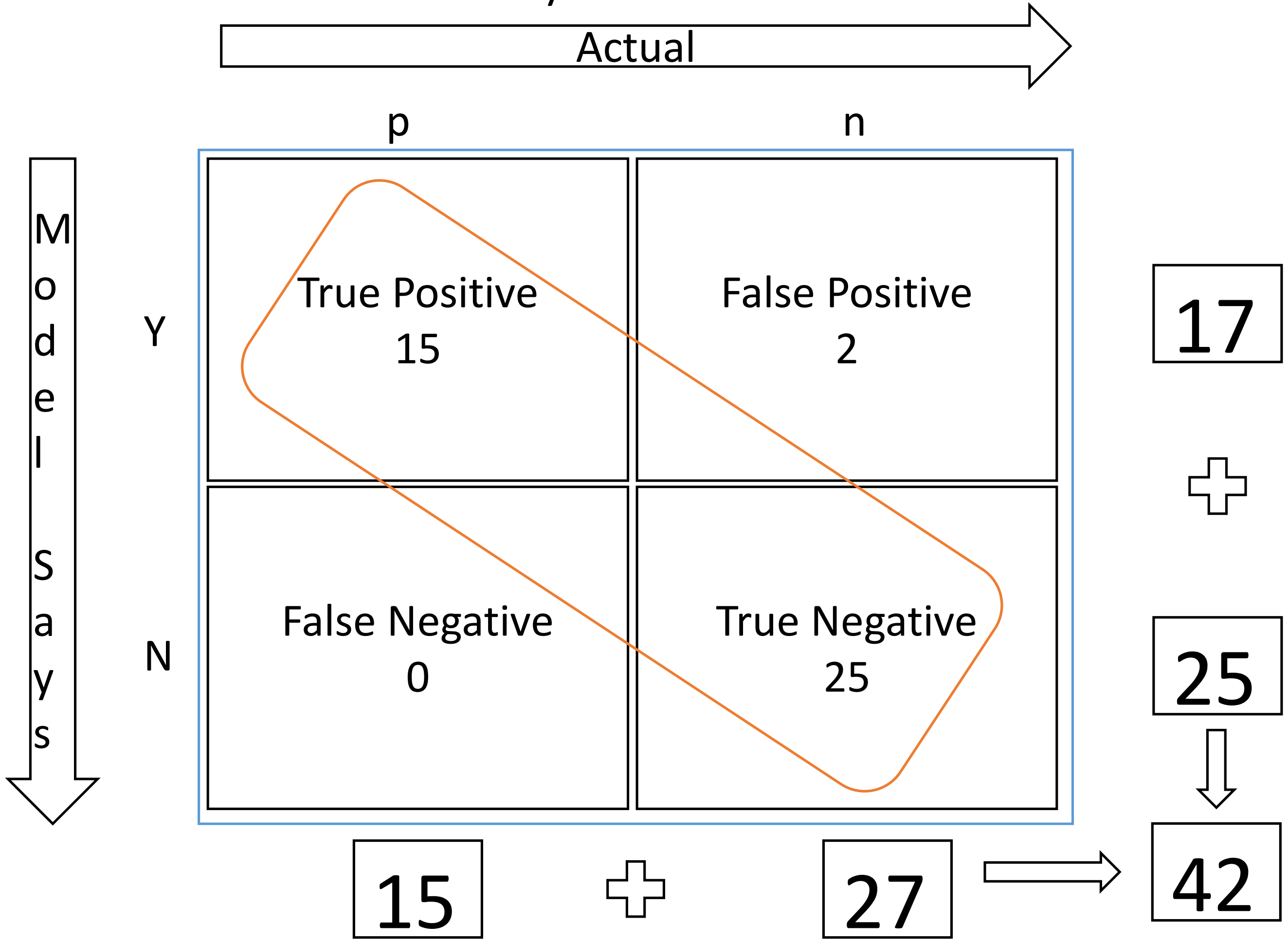


Actual

Model Says

	p	n	
Y	True Positive 15	False Positive 2	17
N	False Negative 0	True Negative 25	25
	15	27	42

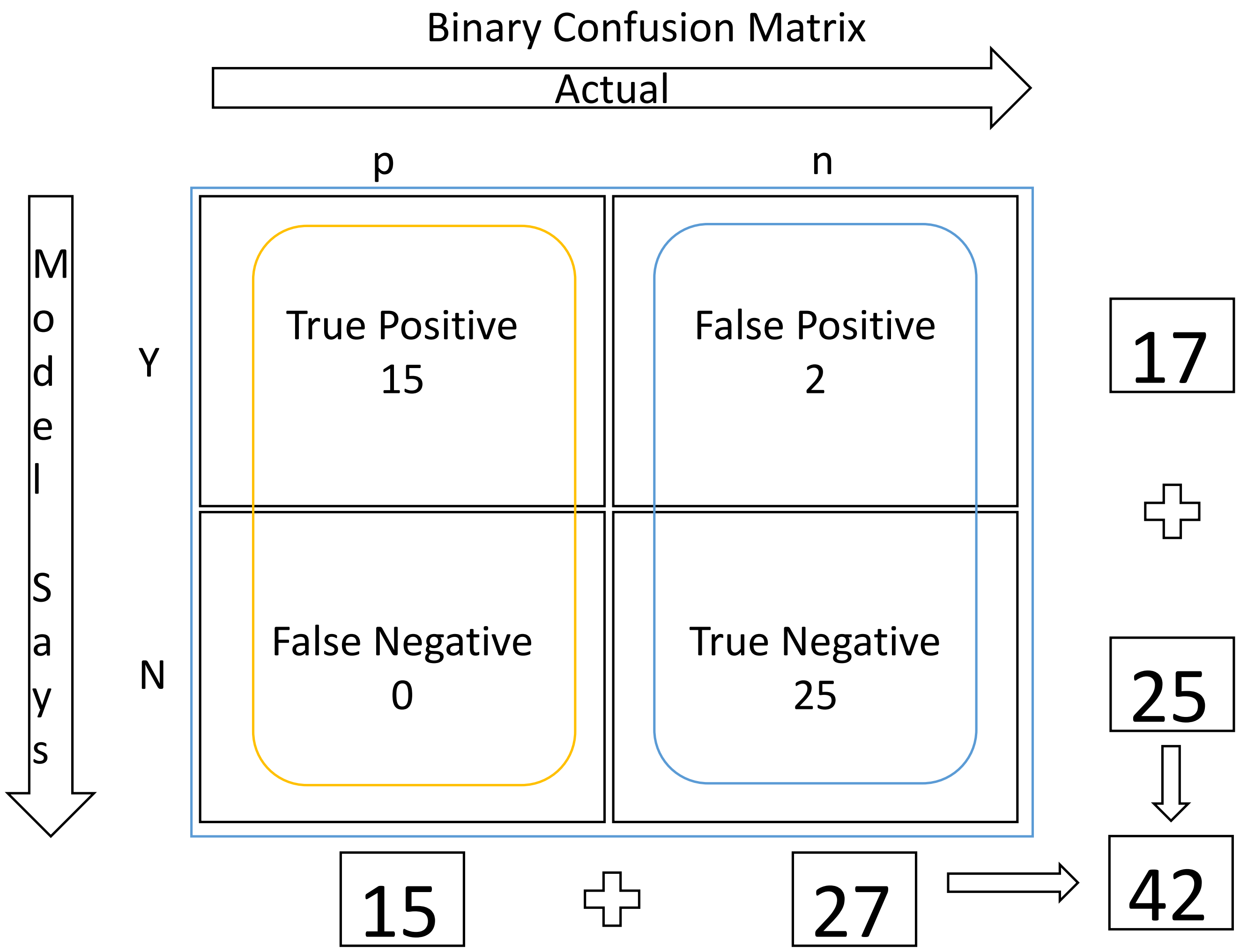
Binary Confusion Matrix



	p	n	
Y	True Positive 15	False Positive 2	17
N	False Negative 0	True Negative 25	25
	15	27	42

$$Accuracy = \frac{TP + TN}{P + N}$$

$$Accuracy = \frac{TP + TN}{P + N}$$



Binary Confusion Matrix

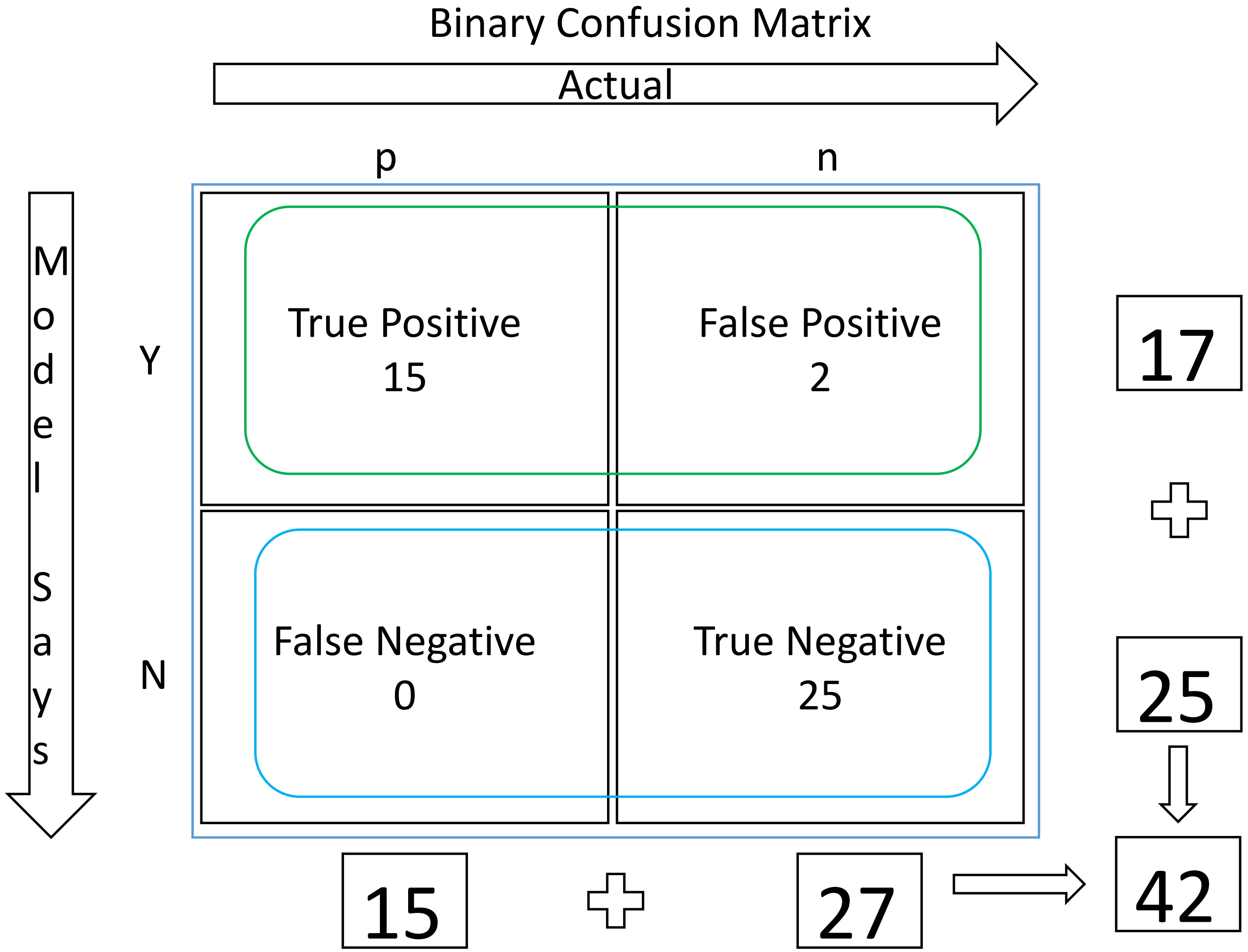
Actual

Model Says

	p	n	
Y	True Positive 15	False Positive 2	17
N	False Negative 0	True Negative 25	25
	15	27	42

$$Sensitivity = TPR = \frac{TP}{TP + FN}$$

$$Specificity = TNR = \frac{TN}{TN + FP}$$



Binary Confusion Matrix

Actual

Model Says

	p	n	
Y	True Positive 15	False Positive 2	17
N	False Negative 0	True Negative 25	25
	15	27	42

17 + 25 → 42

15 + 27 → 42

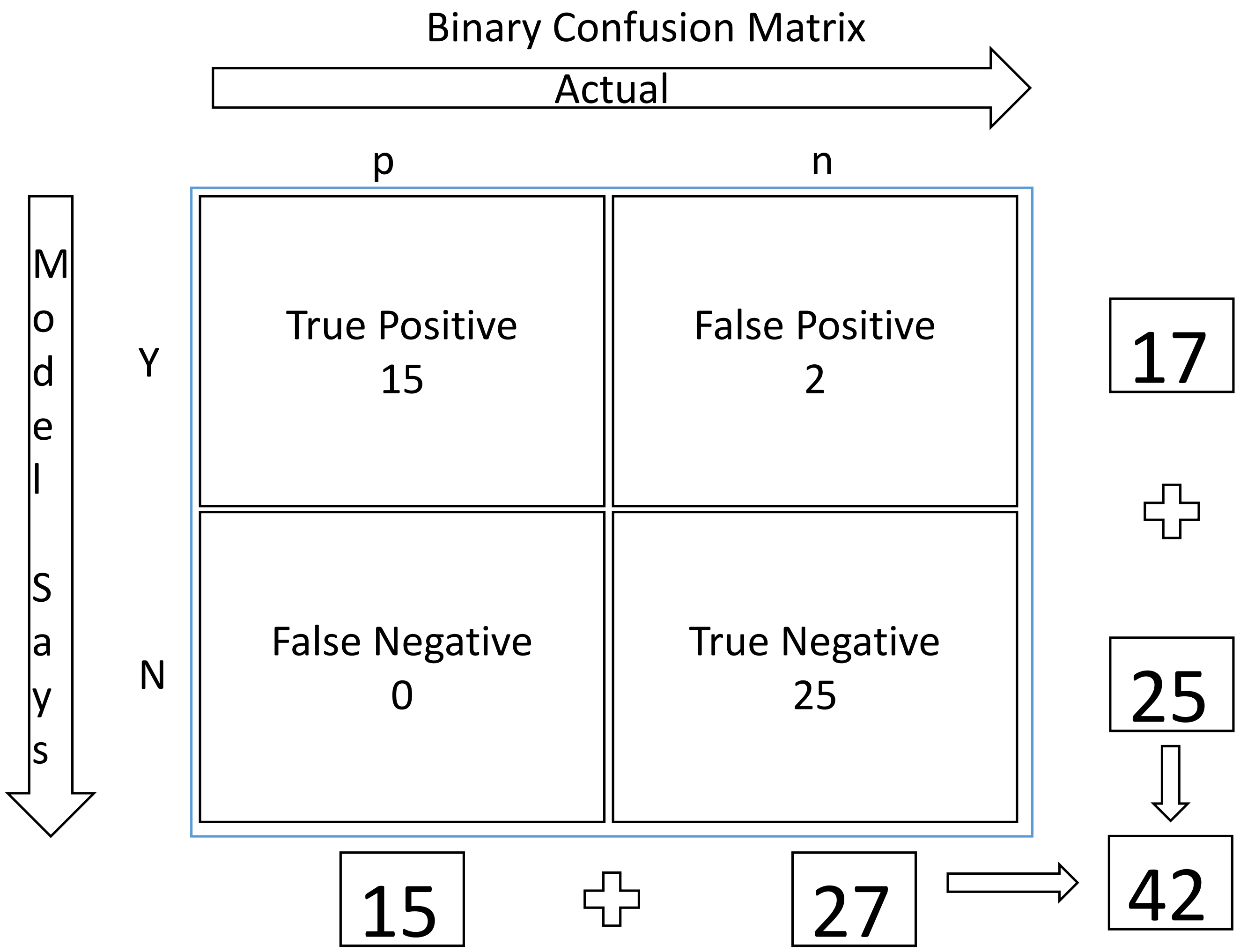
$$Accuracy = \frac{TP + TN}{P + N}$$

$$Sensitivity = TPR = \frac{TP}{TP + FN}$$

$$Specificity = TNR = \frac{TN}{TN + FP}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$



Binary Confusion Matrix

Actual

Model Says

	p	n	
Y	True Positive 15	False Positive 2	17
N	False Negative 0	True Negative 25	25
	15	27	42

$$Accuracy = \frac{TP + TN}{P + N}$$

$$Sensitivity = TPR = \frac{TP}{TP + FN}$$

$$Specificity = TNR = \frac{TN}{TN + FP}$$

$$Precision = \frac{TP}{TP + FP}$$

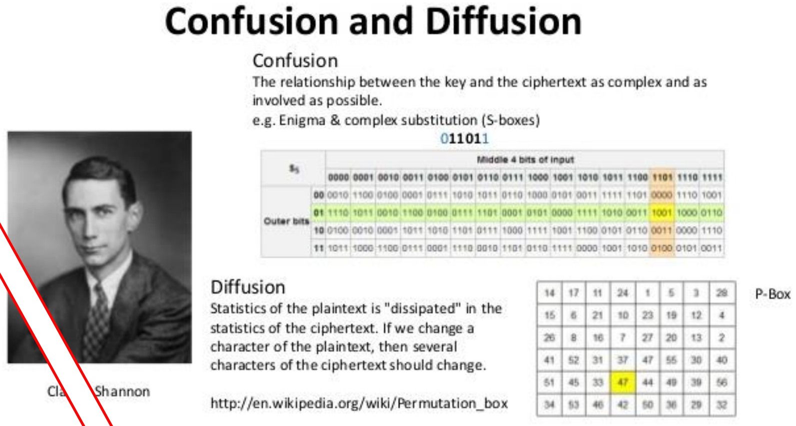
$$Recall = \frac{TP}{TP + FN}$$

$$\text{F-measure} = 2 * \frac{Precision * Recall}{Precision + Recall}$$

Entropy

$$W = \{w : w \in T(v)\}$$

$$\boxed{H = -\sum_{w \in W} p(w) \log_2 p(w)}$$



Confusion and Diffusion

Confusion

The relationship between the key and the ciphertext as complex and as involved as possible.

e.g. Enigma & complex substitution (S-boxes)

011011

S_5		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Cla Shannon

Diffusion

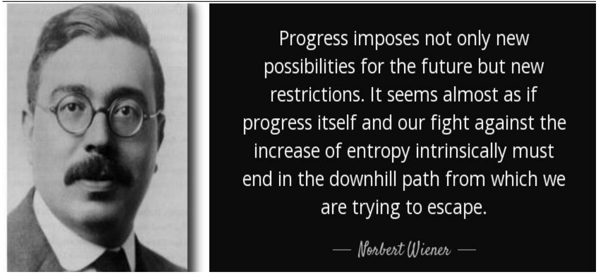
Statistics of the plaintext is "dissipated" in the statistics of the ciphertext. If we change a character of the plaintext, then several characters of the ciphertext should change.

http://en.wikipedia.org/wiki/Permutation_box

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	47	44	49	39	56
34	53	46	42	50	36	29	32

P-Box

$$\boxed{H_t = -\sum_{i=1}^{n} \pi_{it} \ln \pi_{it}.}$$



Progress imposes not only new possibilities for the future but new restrictions. It seems almost as if progress itself and our fight against the increase of entropy intrinsically must end in the downhill path from which we are trying to escape.

— Norbert Wiener —

$$\Delta S = S(set) - S(set|\theta) \Leftrightarrow \Delta H = H(set) - H(set|\theta)$$

$$= -\left[\sum_{i=1}^{N} p_i * \log_{10} p_i\right] - \left\{-\left[\sum_{i=1}^{N} p_{i|\theta} * \log_{10} p_{i|\theta}\right]\right\}$$

$$\sim -\left[\sum_{i=1}^{N} p_i * \log_{10} p_i\right] - \left\{-\left[\sum_{i=1}^{N} p_{i|\theta} * \log_{10} p_{i|\theta}\right]\right\}$$

$$\sim -\left[\sum_{i=1}^{N} p_i * ln\, p_i\right] - \left\{-\left[\sum_{i=1}^{N} p_{i|\theta} * ln\, p_{i|\theta}\right]\right\}$$

As long as you stay consistent with the base of the logs, you are doing the right thing.