Why XOR is so important in cryptography

The following theorem explains why $\oplus$ is so frequently used in cryptography.

Theorem 1. *Let Y be a random variable over $\{0,1\}^n$, and X an independent uniform variable on $\{0,1\}^n$. Then $Z = Y \oplus X$ is uniform on $\{0,1\}^n$.*

Proof. We prove the theorem for $n = 1$. Let $P_0 = Pr\{Y = 0\}$ and $P_1 = Pr\{Y = 1\}$ be the probability distribution of Y. Of course, $P_0 + P_1 = 1$ by definition. Since X is uniform, $1/2$ is the probability of both 0 and 1. Let us now compute the probability distribution of $Z = X \oplus Y$

X	Y	$Z = X \oplus Y$	P(Z)
0	0	0	$P_0/2$
0	1	1	$P_1/2$
1	0	1	$P_0/2$
1	1	0	$P_1/2$

Let us consider the first row, to fix ideas. Since X is independent (of Y), then $P(X = 0; Y = 0) = P(X = 0) \times P(Y = 0) = \frac{1}{2} \times P_0$.

Let us know compute $Pr\{Z = 0\}$. $Pr\{Z = 0\} = Pr\{(X,Y) = (0,0) \vee (X,Y) = (1,1)\}$. The two events are disjoint thus we obtain $Pr\{Z = 0\} = Pr\{(X,Y) = (0,0)\} + Pr\{(X,Y) = (1,1)\} = \frac{P_0}{2} + \frac{P_1}{2} = \frac{1}{2}$.

□