f)

Fakt istnienia Birthday Paradox dał możliwość zaistnienia kryptograficznemu atakowi „Birthday attack”. Funkcja haszująca przerzuca dane dowolnego rozmiaru na skończony zbiór wartości (nazywany haszami). Takie działanie funkcji tworzy możliwość przypasania kilku wartości do jednego hasza – zaistnienie kolizji. Dzięki Birthday Paradox wiemy, że szansa na to, że orginalny i podrobiony plik będą mieć ten sam hash jest dość duża. Birthday attack wykorzystuje ten fakt przez co szansa na udany atak się zwiększa (i/lub czas jego działania się zmniejsza w porównaniu do typowego ataku brute-force).