ملاحظة: رتب أجوبتك في الدفتر حسب ترتيب ورود الأسئلة.

١- (أ) في الفضاء $\mathbb{Z}_2^n$ برهن أن $d(v_1,v_2) \le d(v_1,v_3)+d(v_3,v_2)$ مع ذكر و إثبات الشرط الضروري و الكافي للمساواة.

(ب) إذا كان $v_1 = 101100$ و $v_2 = 110111$ ، فأحسب عدد المتجهات v_3 التي تحقق المساواة في (أ) .

٢- لتكن C شفرة خطية من نوع (n,k,d) . أثبت ما يلي:

(أ) نسبة المعلومة تساوي $\frac{k}{n}$.

(ب) الشفرة تكتشف جميع الأخطاء التي تقع في المتممة $\mathbb{Z}_2^n \setminus C$.

(ت) $k \le n-d+1$.

٣- في شفرة هامينق من نوع $(7,4,3)$:

(أ) أكتب مصفوفة فحص النوعية H .

(ب) احسب المصفوفة المولِّدة G (لاحظ أن H^t تولد $C^\perp$ و أن $C^{\perp\perp} = C$)

(ت) إذا تم استلام الكلمة $w = 0111111$ ، فما هي الكلمة المُرسلة ؟

٤- (أ) صِف نظام RSA ذا المفتاح المُعلن (e,n) ، مبيناً المقادير المعلنة و السرية و الشروط عليها.

(ب) إذا كان $p = 71$ و $q = 83$ ، فأحسب تعمية النص $x = 6001$ ، إذا كان $e = 17$.

(ت) احسب دالة كشف المعمى.

٥- في النظام التآلفي قياس 26 :

(أ) احسب عدد الحروف التي تحقق $e_{(a,b)}(x) = x$ ، إذا كان $(a,b) = (7,4)$.

(ب) احسب رتبة دالة التعمية $e(x) = 3x + 6$ تحت عملية تركيب الدوال ، باعتبارها عنصراً في S_{26} .