الاختبار النهائي — ٤٤٠ رياض — الفصل الثاني ١٤٢٨ - ١٤٢٩

تطبيقات في الجبر

ملاحظة: ① رتب اجابتك في الدفتر حسب ترتيب ورود الاسئلة.
② عليك العناية بوضوح خطواتك وطريقة عرض إجابتك.

١- (أ) لكل x_1، x_2 في $\mathbb{Z}_2^n$، أثبت أن
$$|x_1| + |x_2| \geq |x_1 + x_2|$$
(ب) حدد شرطاً ضرورياً وكافياً للمساواة في المتباينة أعلاه مع الاثبات.
(جـ) إذا كانت $x_1 = 10100$. فجد عدد كلمات x_2 في $\mathbb{Z}_2^5$ بحيث
$$|x_1 + x_2| = |x_1| + |x_2|$$

٢- لتكن $H = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$ هي مصفوفة تحديد الفوضى للشفرة C:
(أ) إحسب المصفوفة المولّدة G
(ب) إحسب بعد الشفرة C وحافتها.
(جـ) إحسب المجموعات المشاركة.
(د) إحسب التصفيف SDA.

٣- لتكن C شفرة طول كلماتها n وحافتها d:
(أ) أثبت أن $|C| \leq \frac{2^n}{\binom{n}{0} + \cdots + \binom{n}{t}}$. حيث $t = \left\lfloor \frac{d-1}{2} \right\rfloor$
(ب) اعط مثالاً على شفرة تحقق المساواة أعلاه مع الشرح.
(جـ) اثبت أن الشفرة التي تحقق المساواة تصحح سوى الاخطاء التي تحقق $|u| \leq t$.

٤- لنعتبر نظام هيل من الدرجة $m = 2$
(أ) احسب عدد المفاتيح في الابجدية العربية التي تحوي 29 حرفاً.
(ب) في الابجدية اللاتينية التي تحوي 26 حرفاً، احسب عدد المفاتيح التي تجعل تعمية الشفي ab هو ab نفسه. (12×26)
(جـ) بين أن نظام تجنير ليس حالة خاصة من نظام هيل.

٥- في نظام RSA الذي مفتاحه المعلن (e, n):
(أ) اثبت ان معرفة $\varphi(n)$ تكافئ معرفة العوامل الأولية للعدد n.
(ب) اذا كان المفتاح المعلن هو $(17, 143)$، فاحسب شفرة الحرف m.
(جـ) لنفس المفتاح المعلن في (ب) إحسب مفتاح كشف المعمى d اذا علمت ان 11 يقسم 143. $(d = 113)$