ملحوظة : ① رتب اجابتك في الدفتر حسب ترتيب ورود الاسئلة
② عليك الاعتناء التام بوضوح الخط وعرض الاجابة

١- لتكن C الشفرة الخطية الحولدة بالمصفوفة

$$S = \{ 110100, 010111, 111010, 011001 \}$$

(أ) اجب المصفوفة الحولدة وحصفوفة تحديد التوءمية 4 3
(ب) اجب المجاميع المشاركة 7
(ج) اجب الصفيف SDA 3
(د) اذا تم استلام الكلمة $w = 000011$ فهل يمكن للشفرة C حساب الكلمة المرسلة ؟ ما هي ؟ 3

٢- (أ) عرّف الشفرة التامة والشفرة من نوع MDS 2 2
(ب) أثبت استحالة وجود شفرة تامة لعددها d_c عدد زوجي.
(ج) هات مثالاً على شفرة تامة غير خطية.
(د) هات مثالاً على شفرة خطية ليست تامة ولا من نوع MDS مع التبرير.

٣- (أ) لتكن C شفرة خطية من نوع (n, k, d) بيث $n > 2^{n-k}$ اثبت وجود غطاء خطأ u وزنه 1 لا يمكن تصويبه.
(ب) صمم شفرة خطية من النوع $(5, 2, 3)$
(ج) هات مثالاً على شفرة C وغطاء خطأ u بحيث $wt(u) \geq \left\lfloor \frac{d_c - 1}{2} \right\rfloor + 1$ يمكن تصويبه بواسطة C.

٤- (أ) اجب عدد المفاتيح الممكنة لنظام هيل قياس 26 من الدرجة $m = 2$ ثم برهن على صحة جوابك. 4 6
(ب) اذا علمت ان تعمية كلمة school هي WUJVKZ في نظام هيل من الدرجة $m = 2$ فما هو المفتاح ؟. 10

٥- (أ) في النظام التتابعي الارجاعي من الدرجة $m = 5$ اذا علمت ان
$(x_i) : 1010111010100011011$
$(y_i) : 0010101110000100101$
فاجب العلاقة الارجاعية 15
(ب) جد كثيرة الحدود المصاحبة للعلاقة الارجاعية في (أ). 5

ملاحظة هامة (١) رتب اجابتك في الدفتر حسب ترتيب ورود الاسئلة
(٢) عليك الاهتمام بوضوح خطك وعرض اجابتك

١- يقال عن شفرة C_2 انها تكافؤ C_1 اذا كانت

$C_2 = \{ uP : u \in C_1 , P$ مصفوفة تبديلية $\}$

(أ) أثبت أن $d_{C_1} = d_{C_2}$

(ب) اذا كان u غط خطأ عكن تصويبه من قبل C_1 ، فهل صحيح انه عكن تصويبه من قبل C_2 ؟ برر اجابتك .

(ج) جد العلاقة بين مصفوفتي تدقيد التوعية H_1 ، H_2 للشفرتين C_1 ، C_2 مع الشرح .

٢- (أ) باستخدام ما درسته حول نظام المعادلات المتجانسة الخطية في الجبر الخطي اثبت أن $\dim C + \dim C^{\perp} = n$ ، حيث $C^{\perp}$ هي الشفرة الثنوية و n طول كلمات الشفرة C .

(ب) اثبت أن شفرة خطية C من نوع (n,k,d) هي MDS اذا وفقط اذا كانت كل $n-k$ من صفوف H مستقلة خطياً . حيث H مصفوفة تدقيد التوعية .

٣- اذا كانت مصفوفة تدقيد التوعية لشفرة C هي

$$H = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

فأجب

(أ) المسافة d_C

(ب) المجموعات المشاركة

(ج) الصفيف SDA .

٤- (أ) عرّف النظام المتنابعي المتناغم

(ب) هات مثالاً على نظام تتابعي غير متناغم مع الشرح مبيناً طريقة التعمية وكشف المعمى

(ج) ما المقصود بطول الدورة في النظام المتناغم ؟ ما هو الحد الأعلى لطول الدورة في النظام الخطي الارجائي ؟

(٥) لنعتبر النظام الافيني في التعمية على الابجدية الانجليزية

(أ) اذا كانت $e_{(a_1,b_1)}$ دالة التعمية بالمفتاح (a_1,b_1) و $e_{(a_2,b_2)}$ دالة التعمية بالمفتاح (a_2,b_2) فأثبت ان التحصيل $e_{(a_1,b_1)} \circ e_{(a_2,b_2)}$ هي دالة تعمية افينية واحسب المفتاح.

(ب) احسب جميع المفاتيح (a,b) بحيث ان $e_{(a,b)} = d_{(a,b)}$ حيث $d_{(a,b)}$ دالة كشف المعمى.

(ج) جد جميع الحروف التي تثبتها دالة التعمية $e_{(5,6)}$ اي جد جميع x بحيث $e_{(5,6)}(x) = x$.

الاختبار النهائي | ٤٤٤ رمز تطبيقات في الجبر | الفصل الصيفي ١٤٤٣ - ١٤٤٤

ملاحظة ① عليك الاعتناء بوضوح خطك وطريقة عرضك للاجابة
② رتب الاجابة في الدفتر حسب ترتيب ورود الاسئلة

① لتكن C شفرة طول كلماتها n وتحوي جميع الكلمات التي عدد الواحدات فيها زوجي.
(أ) جد صيغة لعدد الكلمات في C
(ب) هل يشترط أن تكون C خطية؟ برر اجابتك
(ج) هل يمكن لـ C تصويب اي نمط خطأ وزنه 1؟ برر اجابتك

② (أ) ماهو المقصود بشفرة من نوع MDS؟
(ب) اذا كانت C شفرة بعدها k فأثبت انها من نوع MDS اذا وفقط اذا كان كل k من اعمدة المصفوفة المولدة G مستقلة خطياً.
(ج) هات مثالاً على شفرة غير تافهة من نوع MDS وطول كلماتها 4.

③ لتكن $S=\{1101, 0011, 1110\}$ و $C=\langle S\rangle$
(أ) إحسب المصفوفة المولدة G.
(ب) إحسب مصفوفة تحديد النوعية H.
(ج) إحسب الصنف SDA.
(د) هل يمكن لـ C تصويب الخطأ $u=0001$؟ مع التبرير.

④ (أ) بيّن من خلال مثال وجود نظام تعمية تعدري بحيث أن قيمة معامل الصدفة IC للنص المعمى تساوي نفس القيمة للنص الواضح.
(ب) في النظام التشابهي (السيل) الارجاعي الخطي، اذا علمت ان $m=4$ وأن $x=100110010111$
و $y=001010111010$، فأحسب المصفوفة الناتجة من محاولة تحليل هذا النظام ثم استخدمها لحساب قيم c_i للعلاقة الارجاعية.

الاختبار النهائي — ٤٤٢ رياض — الفصل الصيفي ١٤٤٥

تطبيقات في الجبر

ملاحظة هامة: ① رتب اجابتك في الدفتر حسب ترتيب ورود الاسئلة
② عليك الاعتناء بالخط مع تخصيص هامش اذا دعت الحاجة

1- (أ) اذا كانت C شفرة خطية فأثبت أن $(C^{\perp})^{\perp} = C$ — 4

(ب) بين ان $H = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$ يمكن ان تكون مصفوفة تدقيق — 5

التوعية لشفرة خطية C ثم احسب المصفوفة المولدة G واحسب حافة C.

(ج) احسب المجاميع المشاركة لـ C في (ب) ثم احسب الصفيف SDA. — 4

2- (أ) عرّف الشفرة التامة ؟ — 2

(ب) هات مثالاً على شفرة تامة غير خطية.

(ج) اذا كانت C شفرة تامة خطية من نوع (n,k,d) وكانت $r = \left\lfloor \frac{d-1}{2} \right\rfloor$ فأثبت ان عدد المجاميع المشاركة لـ C يساوي $|B(v,r)|$، حيث $v \in C$. — 4

(د) اذا كانت $w_1, w_2 \in B(v,r)$ حيث $v \in C$ و $w_1 \neq w_2$ فأثبت أن w_1 و w_2 لا يمكن ان يقعا في نفس المجموعة المشاركة. — 4

3- لتكن $C = \{101, 110, 111\}$

(أ) احسب الاخطاء التي تكتشفها C — 3

(ب) احسب الاخطاء التي تصححها C. — 7

(ج) احسب نسبة المعلومة. — 2

4- لتكن A مصفوفة من نوع 2×2 على الحلقة $\mathbb{Z}_{26}$، $B = (b_1, b_2) \in \mathbb{Z}_{26}^2$.

عرّف الدالة $e_{(A,B)}(x_1,x_2) = (y_1,y_2) = (x_1,x_2)A + B$

(أ) ما هو الشرط الضروري والكافي لكي تكون الدالة $e_{(A,B)}$ قابلة للانقلاب؟ — 2

(ب) اذا اعتبرنا $e_{(A,B)}$ دالة تعمية فأحسب عدد المفاتيح الممكنة. — 4

(ج) اذا كانت $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ و $B = (1,1)$ فأثبت استحالة وجود (x_1,x_2) بحيث $e_{(A,B)}(x_1,x_2) = (x_1,x_2)$ — 3

(د) باستخدام A و B اعلاه، جد تعمية النص Success — 4

الاختبار النهائي | ٤٤٤ ربيع | الفصل الثاني ١٤٤٤-١٤٤٥
تطبيقات في الجبر

ملاحظة: ① عليك الاعتناء بوضوح خطك وطريقة عرض اجابتك
② رتب اجابتك في الدفتر حسب ترتيب ورود الاسئلة

١- (أ) في نظام RSA، إذا علمت ان $(x,n)>1$، حيث x هي القيمة العددية لقالب من النص الواضح، فأثبت أن هذا يؤدي الى كسر النظام.

١٥ (ب) اعط وصفاً لكيفية استخدام نظام RSA للتوقيع الالكتروني لرسائل حربية

١٥ (ج) لتكن الشفرة $C=\{101, 110, 001\}$. جد الاخطاء التي يمكن اكتشافها والتي يمكن تصويبها بواسطة C.

٢- (أ) أثبت استقالة وجود شفرة تامة مسافتها عدد زوجي.

٨ (ب) اذا كانت C شفرة تامة مسافتها d، فأثبت مفصلاً أن C تصوب جميع اغلاط الاخطاء u بحيث $wt(u)\leq\left\lfloor\frac{d-1}{2}\right\rfloor$ ولا تصوب سواها.

٩ (ج) اعط مثالاً على شفرة تامة ليست من نوع MDS مع الشرح.

٣- لتكن $C=\langle S\rangle$، حيث $S=\{1010, 0110, 1100\}$

٨ (أ) احسب الصفوفة المولدة لـ C

٤ (ب) احسب صفوفة تحديد النوعية.

٤ (ج) احسب بعد الشفرة k و مسافتها d.

٩ (د) احسب SDA صفيف فك الشفرة القياسي.

٤ (هـ) اذا تم استلام الكلمة $w=1111$ فهل يمكن معرفة الكلمة التي أرسلت؟ ما هي؟

٤- (أ) عرّف نظام التعمية التتابعي.

٢٦ (ب) اثبت أن نظام هيل هو حالة خاصة من النظام التتابعي وذلك ببيان عناصر التعريف المذكورة في (أ).

٩ (ج) احسب عدد المفاتيح المتناظرة في نظام هيل والتي على الصورة $k=\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$.

٨ (د) اشرح كيفية تحليل نظام هيل بمعرفة النص الواضح مع اعطاء مثال

٥- (أ) في نظام RSA اثبت ان تحليل n الى عوامله الاولية يكافئ معرفة الدالة $\phi(n)$.

(ب) استخدم معرفتك من نظرية الزمر لايجاد مولدين مختلفين آخرين للزمرة $\mathbb{Z}_{29}^*$ اذا علمت أن احد المولدات هو 8 .

(ج) في $\mathbb{Z}_n^*$ اذا كان $\log_a b$ موجوداً" فهل صحيح أن $\log_b a$ موجود ؟ برر إجابتك .