

ملاحظة: رتب إجابتك في الدفتر حسب ترتيب ورود الأسئلة.

1. في كلٍ من نظام هيل، فجنير و النظام التبادلي من الدرجة  $m = 3$  ، احسب عدد عناصر فضاء المفاتيح ، إذا كانت أبجدية اللغة تحوي 35 حرفاً. برر إجابتك.
2. ما المقصود بكثيرة الحدود البدائية؟ (أ) أعطِ مثلاً على كثيرة حدود لامختزلة و لكنها غير بدائية. (ب) أثبت أن كل كثيرة حدود لامختزلة من الدرجة  $m = 5$  يجب أن تكون بدائية.
3. في نظام RSA لدينا  $p = 17$  ،  $q = 23$  و  $a = 29$  ، احسب ما يلي:
  - (أ) تعمية النص الواضح top .
  - (ب) قيمة  $b$  التي تعرّف دالة كشف المعمي.
4. لتكن  $C$  شفرة خطية تامة من نوع  $(n, k, d)$ . أثبت أن  $d$  يجب أن يكون فردياً.
5. إذا كانت  $C$  شفرة خطية من نوع  $(n, k, d)$  ، فأثبت ما يلي:
  - (أ) نسبة المعلومة هي  $\frac{k}{n}$  .
  - (ب)  $C$  تكتشف أي نمط خطأ يقع في مُتمماتها و لا تكتشف سواها.
  - (ت)  $d \leq n - k + 1$  .
6. لتكن  $C$  شفرة خطية موكّدة بالمجموعة  $S = \{01011, 00111, 00010, 01001\}$  . احسب المصفوفة  $H$  ، الجاميع المشاركة و الصفيف SDA . إذا تم استلام  $w = 11000$  ، فما هي الكلمة المُرسلة ؟