it sec ex01

1.a)
Confidentiality - Der Dieb könnte durch die persönlichen Unterlagen von Alice gegangen sein,
oder wertvolle Gegenstände gestohlen haben (TV, Laptop, Schmuck)
Integrity - Durch das Stehlen des Laptops kann der Dieb die Möglichkeit bekommen haben sich in ihren Bank Account zu hacken
1.b)
Prevention - Alice könnte sich durch erweiterete Sicherheitsmaßnahmen vor Einbrüchen schützen (z.B. Gesichtserkennung, Sicherheitsschloss).
Außerdem könnte sie ihre wertvollen Unterlagen und Gegenstände zusätzlich in einem Safe aufbewahren.
Detection - Ein Alarmsystem bestehend aus Sensoren und Kameras könnte das Eindringen eines Einbrechers erkennen und die Polizei informieren.
Analysis - Nach einem Einbruch könnte Alice alle ihre Kreditkarten und Bankkonten sperren lassen.
Außerdem könnte sie online nachsehen ob jemand ihren Schmuck weiterverkauft.

2.a)
Keyspace ROT13: Wenn man ROT13 als Rotationverschlüsselung um 13 stellen versteht, dann ist die Größe des Schlüsselraums 1. Denn der Schlüssel ist die 13. Unter der Annahme das eine allgemeine Rotationsverschlüsselung mit Charakterrotation um n Stellen. Dann können alle Buchstaben des Alphabets mal an erster Stelle stehen, also hat man 26 verschiedene Schlüssel. Eine Rotation um 0 Stellen ist trivial, also gibt es 25 sinnvolle Schlüssel.
2.b) 26^3
2.c) 2^256
2.d) k!

3. Eve sollte alle möglichen Paare der drei abgefangen Nachrichten bilden. Diese Paare nimmt sie als Eingabeparameter der XOR-Funktion. Eines der Ergebnisse ist der Schlüssel K. Um herauszufinden welches der Schlüssel K ist, muss sie nun die Ergebnisse mit den ursprünglichen Nachrichten als Eingabeparameter der XOR-Funktion wählen. Wenn eine ursprüngliche Nachricht gefunden wurde, war der erste Eingabeparameter K und die Eingabeparameter der ersten XOR-Operation waren M2 und C2. Damit lässt sich mit M1 = XOR(C1, K) bestimmen.
Anmerkung: K = XOR(M2, C2); C2 = XOR(M2, K)

Break Mono
Mit einem Keyspace von 26! ist die monoalphabetische Substitution schwer über einen Brute Force angriff zu knacken. Trotzdem soll hier ein möglicher Brute Force Angriff skizziert werden: Als Scoring Funktion zum bewerten des Schlüssels kann man eine Wortsuche auf den potenziell entschlüsselten Text starten. Für jedes gefundene Wort vergibt man einen Punkt. Wenn der richtige Schlüssel angewandt wurde erhält man so die meisten passenden Worte.

Praktikabler ist eine Häufigkeitsanalyse der vorkommenden Buchstaben. Man zähle alle Buchstaben im Ciphertext und teilt sie durch die Länge des Texts. Die daraus resultierenden Häufigkeiten kann man mit den Häufigkeiten der Buchstaben von realen englischen Texten vergleichen. Für genauere Analysen können zudem die Bigramme (Buchstabenfolgen der Länge 2), sowie Tri-, Quadri- und Quintgramme hinzugezogen werden

Außerdem sind Klartextangriffe denkbar. Zur Verbesserung des aus der Häufigkeitsanalyse gewonnen Schlüssels können nach Mustern im Klartext gesucht werden. Dazu können Wortlisten eingelesen werden und gemäß eines regulären Ausdrucks codiert werden. Die als sicher angenommenen Subkeys bilden in den regulären Ausdrücken Konstanten.

Break Vig
Vigener kann durch die vorgegebene Schlüssellänge leichter per Brute Force Attack entschlüsselt werden. Als Scoringfunktion dient hier die Häufigkeitsanalyse. Ein Schlüssel wird bewertet anhand des durch diesen Schlüssel entschlüsselten Plaintext. Sind die Häufigkeiten in dem Plaintext nahe an den realen Buchstabenhäufigkeiten, so ist der Schlüssel “gut”.