

\int Skripte **HSLU** Hochschule Luzern

Modul I.BA KRYPT

Musterprüfung/Kompetenznachweis 3

Datum, Zeit und Ort

Name: _____

Bedingungen (für die Prüfung):

Zeit: 90 Minuten
Hilfsmittel: Beliebige schriftliche Unterlagen (Open book), ein beliebiger nicht kommunika-tionsfähiger TR, keine weiteren elektronische Geräte (Handy, Laptop, Tablet usw.).

Bitte beachten Sie:

- Mit Bleistift oder mit **roter** Farbe schreiben ist nicht gestattet.
- Lösungen auf den dafür vorgesehenen Platz eintragen und/oder die angehängten Zusatzblät-ter benutzen.
- Lesen Sie zuerst die Aufgaben, bevor Sie zu lösen anfangen!
- Saubere und deutliche Resultatformulierung (z.B. mit Resultatsatz, dort wo es angebracht ist).
- Unbelegte oder nicht nachvollziehbare Resultate werden nicht berücksichtigt.
- Ungültiges ist sauber durchzustreichen, Mehrfachlösungen werden nicht gewertet.
- Der Lösungsweg muss klar ersichtlich sein.
- Bei Multiple Choice Aufgaben wird falsches Ankreuzen mit Punktabzug bestraft, d.h. im Zweifelsfalle ist es besser die Felder offen zu lassen. Die Summe innerhalb einer solchen Auf-gabe kann aber nicht negativ werden.

Punktzahlen:

maximal: 60

für die Note 6: 50

für die Note 4: 30

Ich wünsche Ihnen viel Glück und viel Erfolg

Josef Schuler

Punkteübersicht:

Aufgabe	Max. Punktzahl	Erreichte Punktzahl	
1)	9		
2)	6		
3)	7		
4)	6		
5)	6		
6)	5		
7)	8		
8)	8		
9)	5		
	-----		Note
Total	60		
	=====	=====	

Aufgabe 1

9 Punkte

Das linke Klartext-Bild ist mit einer Blockchiffre verschlüsselt worden. Das rechte Bild ist die verschlüsselte Version.



- a) [1 P.] Geben Sie einen geeigneten, aktuellen & standardisierten Algorithmus an. _____
- b) [1 P.] Welche minimale Schlüsselgrösse muss verwendet werden? _____
- c) [1 P.] In welchem Modus wurde das obige Bild verschlüsselt? _____
- d) [1 P.] Begründen Sie Ihre Angabe des Modus in Aufgabe c).
- e) [2 P.] Geben Sie je einen (weiteren) Vor- und Nachteil des obigen Modus an.
- Vorteil:
- Nachteil:
- f) [1 P.] Geben Sie einen Modus an, der das Bild besser verschlüsselt.
- g) [1 P.] Das Klartext-Bild soll auf dem Übertragungsweg gegen Verändern geschützt werden. Wie machen Sie das, wenn der oben erwähnte Blockchiffrieralgorithmus benutzt werden soll?
- h) [1 P.] Gibt es für f) eine (symmetrische) Alternative ohne Verwendung eines Blockchiffrieres? Was braucht es dazu? Wie heisst die Konstruktion?

Aufgabe 2**6 Punkte**

Voraussetzungen:

- Alice besitzt den Schlüssel K_1
- Bob besitzt den Schlüssel K_2

Alice möchte Bob die Meldung M verschlüsselt zuschicken. Dabei verwenden Sie das untenstehende Protokoll, das ohne vorgängigen Schlüsselaustausch auskommt. Als Verschlüsselungsoperation wird die Stromchiffre benutzt.

Alice mit K_1	unsichere Leitung	Bob K_2
Alice verschlüsselt die Nachricht M mit ihrem geheimen Schlüssel K_1 .		
	$C_1 = M \oplus K_1$ ----->	
		Bob verschlüsselt die Nachricht C_1 mit seinem geheimen Schlüssel K_2 .
	$C_2 = C_1 \oplus K_2$ <-----	
Alice entschlüsselt die Nachricht C_2 mit ihrem geheimen Schlüssel K_1 .		
	$C_3 = C_2 \oplus K_1$ ----->	
		Bob entschlüsselt die Nachricht C_3 mit seinem geheimen Schlüssel K_2 . $Y = C_3 \oplus K_2 \stackrel{?}{=} M$

- a) [3 P.] Beweisen Sie nun, dass der von Bob zu Letzt berechnete Wert $Y = C_3 \oplus K_2$ tatsächlich gleich der Nachricht M ist.

- b) [3 P.] Es ist nun offensichtlich, dass man nun drei Meldungen statt nur eine Meldung über die Leitung schicken muss. Aufgrund dessen, dass dieses Protokoll nicht implementiert wurde, muss ja noch irgendwo ein anderer Hacken sein. Finden Sie diesen Hacken. **Tipp:** Versetzen Sie sich in Eve, die alle Meldungen abhören kann. Eve hat die Idee, dass sie einfach einmal alle drei über die Leitung geschickten Chiffrate miteinander XOR'ed. Berechnen Sie nun, was dann rauskommt.

Aufgabe 3**7 Punkte**

Sie setzen für eine PIN-Block-Verschlüsselung zwei Typen von Blockchiffren ein:

- Typ A = 256 Bit AES.
- Typ B = Doppel-AES mit je 128 Bit Schlüsselgrösse (Analog einem Doppel-DES).

Die zwei Typen unterziehen Sie nun einer kryptoanalytischen Betrachtung und kommen zu den folgenden Ergebnissen, die Sie nun entsprechend in der Tabelle auswählen und ausfüllen.

Falsches Ankreuzen gibt Punktabzug, die Summe kann aber nicht negativ werden!

Angriff	Typ von Attacke
Table look up	<input type="checkbox"/> Für Typ A und B muss ungefähr der gleiche Aufwand betrieben werden. <input type="checkbox"/> Für Typ A muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input type="checkbox"/> Für Typ B muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input type="checkbox"/> Man kann die Typen bei diesem Angriff gar nicht vergleichen.
Exhaustive Key Search	<input type="checkbox"/> Für Typ A und B muss ungefähr der gleiche Aufwand betrieben werden. <input type="checkbox"/> Für Typ A muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input type="checkbox"/> Für Typ B muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input type="checkbox"/> Man kann die Typen bei diesem Angriff gar nicht vergleichen.
Time-memory-Trade off "meet-in-the-middle"	<input type="checkbox"/> Für Typ A und B muss ungefähr der gleiche Aufwand betrieben werden. <input type="checkbox"/> Für Typ A muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input type="checkbox"/> Für Typ B muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input type="checkbox"/> Man kann die Typen bei diesem Angriff gar nicht vergleichen.

Aufgabe 3, Fortsetzung, resp. Platz für etwaige Berechnungen:


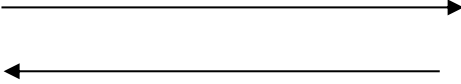

Aufgabe 4


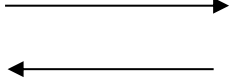

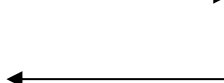

2 + 4 = 6 Punkte

Aufgabe 4.1

2 Punkte

Im Folgenden sind die Abläufe eines nicht angegriffenen und eines angegriffenen Schlüsselaustausch Protokolls gegeben.

Alice		Bob
		
Super, Bob und ich haben nun den gleichen Schlüssel K ausgetauscht!		Super, Alice und ich haben nun den gleichen Schlüssel K ausgetauscht!

Alice		Eve		Bob
				
Super, Bob und ich haben nun den gleichen Schlüssel K ausgetauscht!??				Super, Alice und ich haben nun den gleichen Schlüssel K ausgetauscht!??

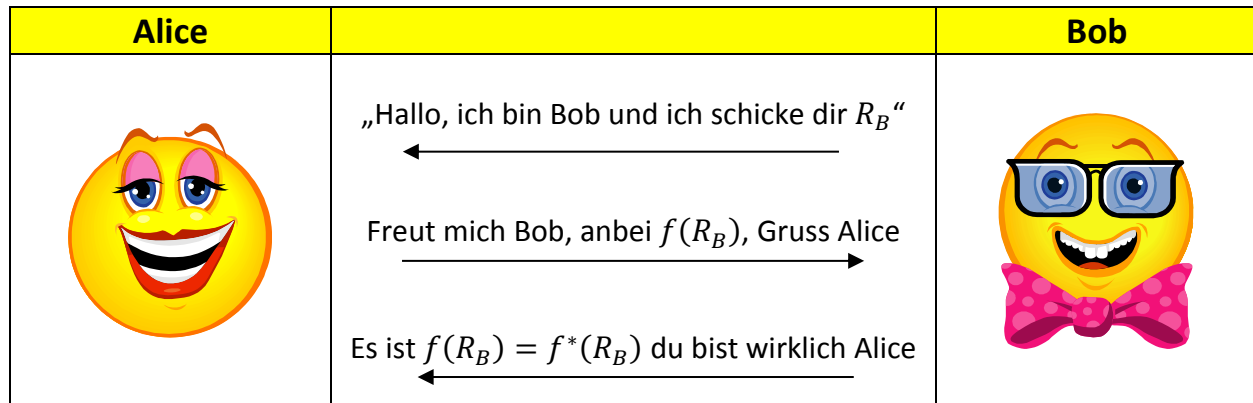
Beantworten Sie die folgenden Fragen (je ½ P.)

- Wie heisst der dargestellte Angriff? _____
- Bei welchem Schlüsselaustausch Protokoll ist der Angriff erfolgreich? _____
- Warum ist der Angriff erfolgreich? _____
- Korrigieren Sie im angegriffenen Protokoll die Aussage „...den gleichen Schlüssel K ausgetauscht!??“, d.h. ersetzen Sie ..., so dass die beiden Aussagen stimmen.

Aufgabe 4.2**4 Punkte**

Im Folgenden ist der Ablauf bei einer Authentisierung gegeben. Im Protokoll werden die folgenden Abkürzungen verwendet:

- R_B = Zufallswert von Bob gewählt; «R» steht für Random.
- $f(R_B)$ der Hashwert von R_B , wobei f eine kryptographisch sichere Hashfunktion (z.B. SHA-2 oder SHA-3) ist. Das ist der Wert den Alice berechnet.
- $f^*(R_B)$ der Hashwert von R_B , wobei f^* die gleiche kryptographisch sichere Hashfunktion wie f ist, aber der Hashwert wird von Bob gerechnet.



Beantworten Sie die folgenden Fragen (je 1 P.)

- Ist das Protokoll „mutual“, wenn JA, dann begründen Sie warum, wenn NEIN, wer authentifiziert sich gegenüber wem?
- Ist die gewählte Funktion (kryptographisch sichere Hashfunktion, z.B. SHA-2 oder SHA-3) ein geeigneter Mechanismus? Wenn JA, warum, wenn NEIN warum nicht, und geben Sie einen geeigneteren an.
- Für eine erfolgreiche einseitige oder gegenseitige Authentisierung fehlt ein wichtiges Element, was für eines?
- Ein wesentliches Element für eine erfolgreiche einseitige oder gegenseitige Authentisierung ist vorhanden, was für eines?

Aufgabe 5**2 + 1 + 3 = 6 Punkte**

Gegeben ist ein RSA System mit den Primzahlen $p = 23$ und $q = 41$ sowie dem öffentlichen Exponenten $e = 9$ und dem geheimen Exponenten $d = 489$.

- a) [2 P.] Zeigen Sie, dass es der öffentliche Exponent $e = 9$ legitim ist.
- b) [1 P.] Zeigen Sie, dass der Exponent d zum Exponent e passt.
- c) [3 P.] Nun verschlüsselt Alice die Meldung $m = ?$ mit dem gegebenen RSA-System und schickt die verschlüsselte Meldung $c = 492$ über die Leitung. Die Angreiferin Eve will die verschlüsselte Meldung c so verändern, dass bei Bob nach dem Entschlüsseln die Meldung $5 \cdot m$ erscheint. Berechnen Sie das neue Chiffre c' , welches Eve erzeugen und an Bob weiterschicken muss.

Aufgabe 5, Fortsetzung, resp. Platz für etwaige Berechnungen:

Aufgabe 6**5 Punkte**

Die 3-stellige Zahl x wird mit der Formel $y \equiv (a \cdot x + b) \bmod N$ verschlüsselt. Die Entschlüsselungsfunktion lautet: $x \equiv a^{-1} \cdot (y - b) \bmod N$. Dabei ist $N = 11 \cdot 23 \cdot 41$ ein Produkt von drei Primzahlen; der Wert N ist öffentlich bekannt. Die Werte a und b bilden in der Form $(a; b)$ den geheimen Schlüssel. Die Werte a und b sind für die Verschlüsselung und Entschlüsselung geeignete Werte aus der Menge $\{2; 3; \dots; N - 1\}$

- a) [1 P.] Begründen Sie, ob es sich hier um eine symmetrische oder asymmetrische Verschlüsselung handelt. **Achtung:** Die Angabe „symmetrisch“ oder „asymmetrisch“ ohne stichhaltige Begründung gibt keine Punkte!
- b) [4 P.] Aus wie vielen möglichen Schlüsseln der Form $(a; b)$ können bei dieser Verschlüsselung ausgewählt werden? Es ist die exakte Zahl anzugeben.

Aufgabe 6, Fortsetzung, resp. Platz für etwaige Berechnungen:

Aufgabe 7**8 Punkte**

Gegeben ist die elliptische Kurve $E: y^2 \equiv x^3 + x + 1$ über \mathbb{Z}_{23} .

- [2 P.] Überprüfen Sie, ob der Punkt (11; 19) auf der Kurve liegt.
- [3 P.] Der Punkt $P(3; 10)$ liegt auf der Kurve. Berechnen Sie die Koordinaten des Punktes $R = 2P$.
- [3 P.] Die Punkte $P(3; 10)$ und $Q(9; 7)$ liegen auf der Kurve. Berechnen Sie die Koordinaten des Punktes $T = P + Q$.

Falls es Ihnen hilft, dürfen Sie zudem die Kehrwerttabelle mod 23 verwenden.

x	1	2	3	4	5	6	7	8	9	10	11
$x^{-1} \bmod 23$	1	12	8	6	14	4	10	3	18	7	21

x	12	13	14	15	16	17	18	19	20	21	22
$x^{-1} \bmod 23$	2	16	5	20	13	19	9	17	15	11	22

Aufgabe 7, Fortsetzung:

Aufgabe 8**8 Punkte**

Alice schickt eine Meldung $M \in \mathbb{Z}_{19}$ verschlüsselt an Bob. Es wird die Verschlüsselungsmethode von Volker-Müller mit Elliptischen Kurven eingesetzt. Aus gewissen Gründen wird die eigentliche Verschlüsselungsoperation ersetzt. Anstatt der XOR-Operation \oplus wird die Addition mod 19 verwendet. Bob hat die folgenden Elemente gewählt...

- ... die elliptische Kurve $E: y^2 \equiv x^3 + 3x + 9$ über \mathbb{Z}_{19} .
- ... den Basispunkt $P(2; 17)$.
- ... den Secret Key $d = 21$.

Alice verschlüsselt die Nachricht $M = 12$. Sollte Alice einen zufälligen Wert generieren müssen, dann können Sie annehmen, dass der Wert 15 gewählt wird.

Alice beginnt den Datenaustausch mit der Meldung (*) = „Hallo Bob, ich möchte dir eine verschlüsselte Meldung schicken.“

Füllen Sie nun die folgende Tabelle aus. Sollten es in der Tabelle zu wenig Platz für allfällige Berechnungen haben, so führen Sie diese bitte auf der nächsten Seite durch.

Sämtliche Operationen mit den Punkten können mit der Tabelle am Schluss der Prüfung nachgeschaut werden.

Die Vorlage für die Aufgabe 8 befindet sich auf der nächsten Seite. Sollten Sie Platz für etwaige Berechnungen brauchen, verwenden Sie zunächst den untenstehenden freien Platz. Ggf. ein Zusatzblatt verwenden.

Vorlage für die Aufgabe 8:

Alice	unsichere Leitung	Bob
	(*) ----->	
	$K_{pub} = (p, a, b, q, P, Q)$ <-----	Bob schickt $K_{pub} = (p, a, b, q, P, Q)$
K_{pub} in der vorgegebenen Reihenfolge angeben. $= (p, a, b, q, P, Q)$ $= ($		
Verschlüsselt Meldung $M = 12$		
	Meldung notieren ----->	
		Entschlüsselung

Aufgabe 9**5 Punkte**

Sie nutzen eine Sicherheitsapplikation, die Zertifikate für die Authentifizierung des Kommunikationspartners verwendet. Beim Versuch, sich mit einem neuen Partner zu verbinden, erhalten Sie eine Fehlermeldung, wonach das Root-CA-Zertifikat, das dem Zertifikat des Verbindungspartners zugrunde liegt, nicht vertrauenswürdig sei. Sie haben die Möglichkeit, den Verbindungsaufbau abubrechen oder das Root-CA-Zertifikat zu installieren. Die Sicherheitsapplikation zeigt Ihnen den Inhalt und weitere Eigenschaften des Root-CA-Zertifikats an. Sie entscheiden sich, das Root-CA-Zertifikat installieren.

a) Was müssen Sie tun, bevor Sie das Zertifikat installieren. Beschreiben Sie den Vorgang stichwortartig (3 Punkte).

b) Die oben beschriebene Fehlermeldung tritt glücklicherweise nur selten auf, weil die Prüfung des Zertifikats des Verbindungspartners in der Regel ohne Fehler durchgeführt werden kann. Beschreiben Sie in wenigen Worten, wie die Sicherheitsapplikation (oder das Betriebssystem) die Echtheit des Zertifikats des Verbindungspartners überprüft (1 Punkt). Welche Rolle spielt dabei der so genannte Trust Anchor (1 Punkt).

Anhang zur Aufgabe 8

P(0; 3)		P(0; 16)		P(2; 2)		P(2; 17)
1·P = (0; 3)		1·P = (0; 16)		1·P = (2; 2)		1·P = (2; 17)
2·P = (5; 4)		2·P = (5; 15)		2·P = (16; 12)		2·P = (16; 7)
3·P = (11; 10)		3·P = (11; 9)		3·P = (5; 4)		3·P = (5; 15)
4·P = (15; 3)		4·P = (15; 16)		4·P = (4; 3)		4·P = (4; 16)
5·P = (4; 16)		5·P = (4; 3)		5·P = (18; 9)		5·P = (18; 10)
6·P = (3; 11)		6·P = (3; 8)		6·P = (15; 3)		6·P = (15; 16)
7·P = (2; 17)		7·P = (2; 2)		7·P = (11; 9)		7·P = (11; 10)
8·P = (9; 10)		8·P = (9; 9)		8·P = (12; 5)		8·P = (12; 14)
9·P = (16; 12)		9·P = (16; 7)		9·P = (3; 11)		9·P = (3; 8)
10·P = (12; 14)		10·P = (12; 5)		10·P = (0; 16)		10·P = (0; 3)
11·P = (18; 9)		11·P = (18; 10)		11·P = (9; 9)		11·P = (9; 10)
12·P = (18; 10)		12·P = (18; 9)		12·P = (9; 10)		12·P = (9; 9)
13·P = (12; 5)		13·P = (12; 14)		13·P = (0; 3)		13·P = (0; 16)
14·P = (16; 7)		14·P = (16; 12)		14·P = (3; 8)		14·P = (3; 11)
15·P = (9; 9)		15·P = (9; 10)		15·P = (12; 14)		15·P = (12; 5)
16·P = (2; 2)		16·P = (2; 17)		16·P = (11; 10)		16·P = (11; 9)
17·P = (3; 8)		17·P = (3; 11)		17·P = (15; 16)		17·P = (15; 3)
18·P = (4; 3)		18·P = (4; 16)		18·P = (18; 10)		18·P = (18; 9)
19·P = (15; 16)		19·P = (15; 3)		19·P = (4; 16)		19·P = (4; 3)
20·P = (11; 9)		20·P = (11; 10)		20·P = (5; 15)		20·P = (5; 4)
21·P = (5; 15)		21·P = (5; 4)		21·P = (16; 7)		21·P = (16; 12)
22·P = (0; 16)		22·P = (0; 3)		22·P = (2; 17)		22·P = (2; 2)
23·P = \emptyset		23·P = \emptyset		23·P = \emptyset		23·P = \emptyset

P(3; 8)		P(3; 11)		P(4; 3)		P(4; 16)
1·P = (3; 8)		1·P = (3; 11)		1·P = (4; 3)		1·P = (4; 16)
2·P = (18; 9)		2·P = (18; 10)		2·P = (12; 5)		2·P = (12; 14)
3·P = (4; 16)		3·P = (4; 3)		3·P = (9; 10)		3·P = (9; 9)
4·P = (0; 16)		4·P = (0; 3)		4·P = (11; 10)		4·P = (11; 9)
5·P = (2; 2)		5·P = (2; 17)		5·P = (5; 15)		5·P = (5; 4)
6·P = (12; 14)		6·P = (12; 5)		6·P = (2; 2)		6·P = (2; 17)
7·P = (15; 3)		7·P = (15; 16)		7·P = (18; 9)		7·P = (18; 10)
8·P = (5; 15)		8·P = (5; 4)		8·P = (3; 11)		8·P = (3; 8)
9·P = (9; 9)		9·P = (9; 10)		9·P = (0; 3)		9·P = (0; 16)
10·P = (16; 12)		10·P = (16; 7)		10·P = (15; 16)		10·P = (15; 3)
11·P = (11; 10)		11·P = (11; 9)		11·P = (16; 7)		11·P = (16; 12)
12·P = (11; 9)		12·P = (11; 10)		12·P = (16; 12)		12·P = (16; 7)
13·P = (16; 7)		13·P = (16; 12)		13·P = (15; 3)		13·P = (15; 16)
14·P = (9; 10)		14·P = (9; 9)		14·P = (0; 16)		14·P = (0; 3)
15·P = (5; 4)		15·P = (5; 15)		15·P = (3; 8)		15·P = (3; 11)
16·P = (15; 16)		16·P = (15; 3)		16·P = (18; 10)		16·P = (18; 9)
17·P = (12; 5)		17·P = (12; 14)		17·P = (2; 17)		17·P = (2; 2)
18·P = (2; 17)		18·P = (2; 2)		18·P = (5; 4)		18·P = (5; 15)
19·P = (0; 3)		19·P = (0; 16)		19·P = (11; 9)		19·P = (11; 10)
20·P = (4; 3)		20·P = (4; 16)		20·P = (9; 9)		20·P = (9; 10)
21·P = (18; 10)		21·P = (18; 9)		21·P = (12; 14)		21·P = (12; 5)
22·P = (3; 11)		22·P = (3; 8)		22·P = (4; 16)		22·P = (4; 3)
23·P = \emptyset		23·P = \emptyset		23·P = \emptyset		23·P = \emptyset

P(5; 4)		P(5; 15)		P(9; 9)		P(9; 10)
1·P = (5; 4)		1·P = (5; 15)		1·P = (9; 9)		1·P = (9; 10)
2·P = (15; 3)		2·P = (15; 16)		2·P = (2; 17)		2·P = (2; 2)
3·P = (3; 11)		3·P = (3; 8)		3·P = (0; 16)		3·P = (0; 3)
4·P = (9; 10)		4·P = (9; 9)		4·P = (16; 7)		4·P = (16; 12)
5·P = (12; 14)		5·P = (12; 5)		5·P = (3; 11)		5·P = (3; 8)
6·P = (18; 10)		6·P = (18; 9)		6·P = (5; 15)		6·P = (5; 4)
7·P = (16; 7)		7·P = (16; 12)		7·P = (12; 5)		7·P = (12; 14)
8·P = (2; 2)		8·P = (2; 17)		8·P = (4; 16)		8·P = (4; 3)
9·P = (4; 3)		9·P = (4; 16)		9·P = (11; 9)		9·P = (11; 10)
10·P = (11; 9)		10·P = (11; 10)		10·P = (18; 10)		10·P = (18; 9)
11·P = (0; 16)		11·P = (0; 3)		11·P = (15; 3)		11·P = (15; 16)
12·P = (0; 3)		12·P = (0; 16)		12·P = (15; 16)		12·P = (15; 3)
13·P = (11; 10)		13·P = (11; 9)		13·P = (18; 9)		13·P = (18; 10)
14·P = (4; 16)		14·P = (4; 3)		14·P = (11; 10)		14·P = (11; 9)
15·P = (2; 17)		15·P = (2; 2)		15·P = (4; 3)		15·P = (4; 16)
16·P = (16; 12)		16·P = (16; 7)		16·P = (12; 14)		16·P = (12; 5)
17·P = (18; 9)		17·P = (18; 10)		17·P = (5; 4)		17·P = (5; 15)
18·P = (12; 5)		18·P = (12; 14)		18·P = (3; 8)		18·P = (3; 11)
19·P = (9; 9)		19·P = (9; 10)		19·P = (16; 12)		19·P = (16; 7)
20·P = (3; 8)		20·P = (3; 11)		20·P = (0; 3)		20·P = (0; 16)
21·P = (15; 16)		21·P = (15; 3)		21·P = (2; 2)		21·P = (2; 17)
22·P = (5; 15)		22·P = (5; 4)		22·P = (9; 10)		22·P = (9; 9)
23·P = \emptyset		23·P = \emptyset		23·P = \emptyset		23·P = \emptyset

P(11; 9)		P(11; 10)		P(12; 5)		P(12; 14)
1·P = (11; 9)		1·P = (11; 10)		1·P = (12; 5)		1·P = (12; 14)
2·P = (3; 8)		2·P = (3; 11)		2·P = (11; 10)		2·P = (11; 9)
3·P = (16; 7)		3·P = (16; 12)		3·P = (2; 2)		3·P = (2; 17)
4·P = (18; 9)		4·P = (18; 10)		4·P = (3; 11)		4·P = (3; 8)
5·P = (9; 10)		5·P = (9; 9)		5·P = (15; 16)		5·P = (15; 3)
6·P = (4; 16)		6·P = (4; 3)		6·P = (16; 12)		6·P = (16; 7)
7·P = (5; 4)		7·P = (5; 15)		7·P = (0; 16)		7·P = (0; 3)
8·P = (0; 16)		8·P = (0; 3)		8·P = (18; 10)		8·P = (18; 9)
9·P = (15; 16)		9·P = (15; 3)		9·P = (5; 4)		9·P = (5; 15)
10·P = (2; 2)		10·P = (2; 17)		10·P = (9; 9)		10·P = (9; 10)
11·P = (12; 5)		11·P = (12; 14)		11·P = (4; 16)		11·P = (4; 3)
12·P = (12; 14)		12·P = (12; 5)		12·P = (4; 3)		12·P = (4; 16)
13·P = (2; 17)		13·P = (2; 2)		13·P = (9; 10)		13·P = (9; 9)
14·P = (15; 3)		14·P = (15; 16)		14·P = (5; 15)		14·P = (5; 4)
15·P = (0; 3)		15·P = (0; 16)		15·P = (18; 9)		15·P = (18; 10)
16·P = (5; 15)		16·P = (5; 4)		16·P = (0; 3)		16·P = (0; 16)
17·P = (4; 3)		17·P = (4; 16)		17·P = (16; 7)		17·P = (16; 12)
18·P = (9; 9)		18·P = (9; 10)		18·P = (15; 3)		18·P = (15; 16)
19·P = (18; 10)		19·P = (18; 9)		19·P = (3; 8)		19·P = (3; 11)
20·P = (16; 12)		20·P = (16; 7)		20·P = (2; 17)		20·P = (2; 2)
21·P = (3; 11)		21·P = (3; 8)		21·P = (11; 9)		21·P = (11; 10)
22·P = (11; 10)		22·P = (11; 9)		22·P = (12; 14)		22·P = (12; 5)
23·P = \emptyset		23·P = \emptyset		23·P = \emptyset		23·P = \emptyset

P(15; 3)		P(15; 16)		P(16; 7)		P(16; 12)
1·P = (15; 3)		1·P = (15; 16)		1·P = (16; 7)		1·P = (16; 12)
2·P = (9; 10)		2·P = (9; 9)		2·P = (4; 16)		2·P = (4; 3)
3·P = (18; 10)		3·P = (18; 9)		3·P = (15; 16)		3·P = (15; 3)
4·P = (2; 2)		4·P = (2; 17)		4·P = (12; 14)		4·P = (12; 5)
5·P = (11; 9)		5·P = (11; 10)		5·P = (0; 3)		5·P = (0; 16)
6·P = (0; 3)		6·P = (0; 16)		6·P = (9; 9)		6·P = (9; 10)
7·P = (4; 16)		7·P = (4; 3)		7·P = (3; 11)		7·P = (3; 8)
8·P = (16; 12)		8·P = (16; 7)		8·P = (11; 9)		8·P = (11; 10)
9·P = (12; 5)		9·P = (12; 14)		9·P = (18; 9)		9·P = (18; 10)
10·P = (3; 8)		10·P = (3; 11)		10·P = (5; 4)		10·P = (5; 15)
11·P = (5; 15)		11·P = (5; 4)		11·P = (2; 2)		11·P = (2; 17)
12·P = (5; 4)		12·P = (5; 15)		12·P = (2; 17)		12·P = (2; 2)
13·P = (3; 11)		13·P = (3; 8)		13·P = (5; 15)		13·P = (5; 4)
14·P = (12; 14)		14·P = (12; 5)		14·P = (18; 10)		14·P = (18; 9)
15·P = (16; 7)		15·P = (16; 12)		15·P = (11; 10)		15·P = (11; 9)
16·P = (4; 3)		16·P = (4; 16)		16·P = (3; 8)		16·P = (3; 11)
17·P = (0; 16)		17·P = (0; 3)		17·P = (9; 10)		17·P = (9; 9)
18·P = (11; 10)		18·P = (11; 9)		18·P = (0; 16)		18·P = (0; 3)
19·P = (2; 17)		19·P = (2; 2)		19·P = (12; 5)		19·P = (12; 14)
20·P = (18; 9)		20·P = (18; 10)		20·P = (15; 3)		20·P = (15; 16)
21·P = (9; 9)		21·P = (9; 10)		21·P = (4; 3)		21·P = (4; 16)
22·P = (15; 16)		22·P = (15; 3)		22·P = (16; 12)		22·P = (16; 7)
23·P = \emptyset		23·P = \emptyset		23·P = \emptyset		23·P = \emptyset

P(18; 9)		P(18; 10)				
1·P = (18; 9)		1·P = (18; 10)				
2·P = (0; 16)		2·P = (0; 3)				
3·P = (12; 14)		3·P = (12; 5)				
4·P = (5; 15)		4·P = (5; 4)				
5·P = (16; 12)		5·P = (16; 7)				
6·P = (11; 9)		6·P = (11; 10)				
7·P = (9; 10)		7·P = (9; 9)				
8·P = (15; 16)		8·P = (15; 3)				
9·P = (2; 17)		9·P = (2; 2)				
10·P = (4; 3)		10·P = (4; 16)				
11·P = (3; 11)		11·P = (3; 8)				
12·P = (3; 8)		12·P = (3; 11)				
13·P = (4; 16)		13·P = (4; 3)				
14·P = (2; 2)		14·P = (2; 17)				
15·P = (15; 3)		15·P = (15; 16)				
16·P = (9; 9)		16·P = (9; 10)				
17·P = (11; 10)		17·P = (11; 9)				
18·P = (16; 7)		18·P = (16; 12)				
19·P = (5; 4)		19·P = (5; 15)				
20·P = (12; 5)		20·P = (12; 14)				
21·P = (0; 3)		21·P = (0; 16)				
22·P = (18; 10)		22·P = (18; 9)				
23·P = \emptyset		23·P = \emptyset				