جامعة المنارة

كلية الهندسة

قسم المعلوماتية

Information System Security

أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

الأربعاء18/11/2024

عناوين المحاضرة الرابعة

- خوارزمية RSA(Rivest Shamir et Adleman)
  - ✓ الأسس الرياضية لخوارزمية RSA
  - ✓ آلية عمل الخوارزمية
  - ✓ أمن الخوارزمية
  - ✓ استخداماتها الحالية
- خوارزمية ديفي هيلمان لتوزيع المفاتيح DH(Diffie-Hellman)
  - ✓ أهمية الخوارزمية
  - ✓ آلية عمل الخوارزمية
  - ✓ أمن الخوارزمية

مقدمة عن خوارزمية RSA

- هي عبارة عن خوارزمية **تشفير غير متناظر**، وضعت من قبل Ronald L. **R**ivest, Adi **S**hamir and Leonard M. **A**dleman في عام1977, و هي تعتمد على عدة أسس رياضية في نظرية الأعداد.
- هي عبارة عن نظام تعمية كتلي
- دخله وخرجه عبارة عن أرقام صحيحة تتراوح قيمتها بين 0 – (n-1) من أجل قيمة لـ n ، الحجم النموذجي لـ n هي 1024 خانة ثنائية
- تعتمد هذه الخوارزمية على صعوبة تحليل الأعداد الكبيرة إلى عواملها الأولية. هذه الأرقام الكبيرة هي عبارة عن ناتج من ضرب عددين أوليين كبيرين.

أسس رياضية لخوارزمية RSA

❖ **الأعداد الأولية فيما بينها:**

✓ نقول عن عددين أنهما عددين أوليين فيما بينهما إذا كان القاسم المشترك الأكبر لهما هو الواحد

مثال: العددين 21, 10 هما عددين أوليين فيما بينهما لأن 10 يقبل القسمة على 1,2,5,10 و العدد 21 يقبل القسمة على 1,3,7,21 أي لا يوجد بينها معامل مشترك سوى الواحد.

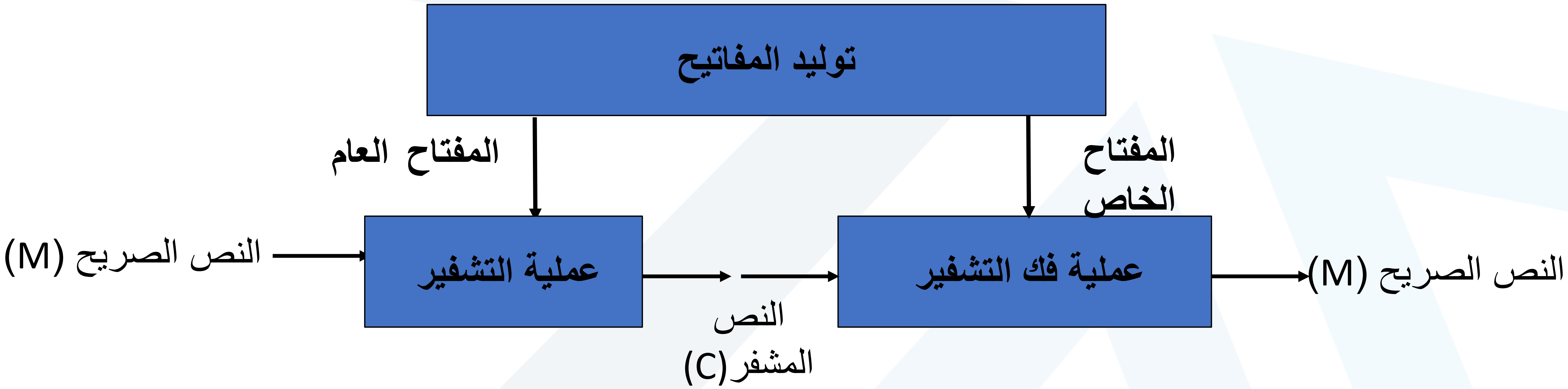
❖ **التابع $\phi(n)$:**

✓ يعرف التابع $\phi(n)$ على أنه **عدد** الأعداد الأقل من n و التي **تكون أولية مع (n)**

مثال: $\phi(6)=2$. لأن الأعداد الأقل من 6 هي 1,2,3,4,5 لكن نلاحظ أن 1,5 هما فقط العددين الأوليين مع العدد 6 بينما 2,4 يشتركان مع العدد 6 بالمعامل 2 و العدد 3 يشترك مع 6 بالمعامل 3

❖ من أجل **أي عدد أولي n** يكون: $\phi(n)=n-1$ **مثال:** $\phi(7)=6$

المخطط الصندوقي لخوارزمية RSA



توليد المفاتيح (Key Generation)
(المفتاح العام و المفتاح الخاص)

1. نختار عددين أوليين كبيرين (q , p) و بحيث $p \neq q$

2. نحسب : $n = p \times q$

3. نحسب : $\phi(n) = (p-1) \times (q-1)$

4. نختار عدد صحيح (e) بحيث يكون : $\gcd(\phi(n), e) = 1; \quad 1 < e < \phi(n)$

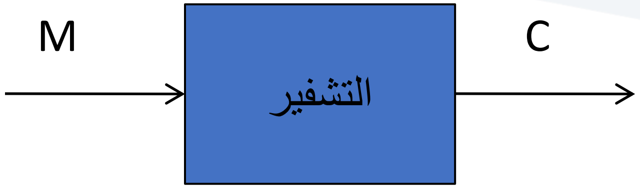
فيكون المفتاح العام :
$K_{pub} = \{e, n\}$

5. نحسب (d) : $d \equiv e^{-1} \bmod \phi(n) \rightarrow d \times e \equiv 1 \bmod \phi(n)$

فيكون المفتاح الخاص : $K_{pri} = \{d, n\}$

عملية التشفير (Encryption)

يستخدم المفتاح العام للمستقبل



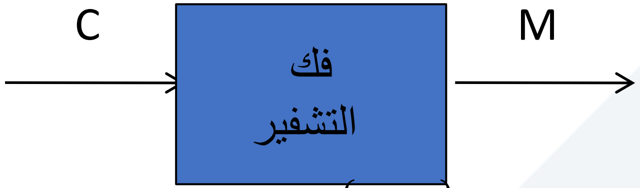
$$K_{pub} = \{e, n\}$$

النص الصريح: $M<n$

النص المشفر : $C = M^{e} \bmod(n)$

عملية فك التشفير (Decryption)

يستخدم المفتاح الخاص للمستقبل



$$K_{pri} = \{d, n\}$$

النص المشفر: C

النص الصريح: $M = C^{d} \bmod(n)$

أمن الخوارزمية RSA (1/2)

❖ توجد عدة هجومات نذكر منها :

➢ الهجوم الأعمى (Brute force):

يتضمن تجريب جميع المفاتيح الممكنة،   الحل يكون باستخدام مفاتيح طويلة(قيم e,d)

➢ الهجوم الرياضي (Mathematical Attack):

عادة يتبع الهجوم الرياضي ما يلي: (المفتاح العام معروف من قبل المهاجم)

1. تحليل n إلى عددين أوليين (p , q)بحيث n=p*q
2. حساب تابع أولر $\phi(n) = (p-1)\times(q-1)$
3. إيجاد المفتاح الخاص بمعرفة e $d \equiv e^{-1} \bmod \phi(n)$

يمكن مقاومة هذا الهجوم عن طريق تكبير قيمة n كثيراً ليصعب تحليلها إلى العوامل الأولية .

مثال

اختار رقمين أوليين كبيرين p,q عشوائيين و مختلفين عن بعضهما .

لدينا هنا مثال عن أعداد أولية ولدت باستخدام اختبار Rabin-Miller primality tests

p

1213107243921127189732367153161244042847242763370141092563454931230196437304208561932419736532241686654101705736136521417171171379797429933487106282980354 1

q

120275242554787488859562207937345121287333878036820754336538999839551798509887978998691469008091316111533468170508320960221601463663463918124709871054152 33

باستخدام هذين الرقمين نحسب $\phi(n)$ و n

n

1459067680075833232301869393490706352924018723753571643995818710198734387990053589383695714026
7014980212181808629246742282815702292207674690654340122488967247240792696998710058129010319931
7858753663710862357656510507883714297115637342788911463535102712032765166518411726859837988672
111837205085526346618740053

φ(n)

1459067680075833232301869393490706352924018723753571643995818710198734387990053589383695714026
7014980212181808629246742282815702292207674690654340122488964831381123227996631730139777785236
5301547848273478871297222058587457152891606459269718119268971163555070802643999529549644116811
947516513938184296683521280

أمن الخوارزمية RSA (2/2)

➢ أمثلة عن كسر الخوارزمية بالهجوم الرياضي :

العدد التقريبي للبتات الثنائية	تاريخ الكسر
332	1991
365	1992
398	1993
428	1994
465	1999
512	1999
664	2005

➢ يعد المفتاح ذو الطول الذي يتراوح [2048-4096] بت آمن .

الاستخدامات الحالية لخوارزمية RSA

- تستخدم في WEB Browsers عند Microsoft, Netscape

- تستخدم في عدة منتجات برمجية تجارية وفي أنظمة التشغيل مثل Microsoft, Apple, sun, Novell

- تستخدم أيضاً في العتاد الصلب كالهواتف الآمنة وبطاقات شبكات الايثرنت, وعلى البطاقات الذكية.

- كما تستخدم في أغلب بروتوكولات الاتصالات الآمنة عبر الإنترنت مثل S/MIME و SSL, ...

أهمية خوارزمية ديفي هيلمان DH(Diffie-Hellman)

تبادل المفتاح السري (المتناظر) بين طرفين (أليس و بوب) يكون باتباع الخطوات الآتية :

1. يولد بوب المفتاح المتناظر Ks
2. يشفر بوب المفتاح المتناظر Ks باستخدام المفتاح العام لأليس
3. تفك أليس التشفير باستخدام المفتاح الخاص لها، و تحصل على المفتاح المتناظر Ks
4. يشفر كل من بوب و أليس المعلومات باستخدام المفتاح المتناظر و أية خوارزمية تشفير متناظر (DES,3DES...)

المشكلة هنا : ماذا لو أن أحد الطرفين لا يملك مفتاحاً عاماً

الحل: استخدام خوارزمية ديفي هيلمان لتبادل المفاتيح لأنها تسمح بتوليد مفتاح سري بين طرفين دون وجود مسبق لمفتاح عام

الفكرة العامة لخوارزمية ديفي هيلمان

تعتمد على أن الطرفين يتبادلان معلومات ، هذه المعلومات تسمح بتوليد مفتاح متناظر بشكل آمن، يستخدم لتشفير المعلومات المتبادل بينهما

آلية عمل خوارزمية ديفي هيلمان لتبادل المفاتيح(1/3)

1. يتفق الطرفان (أليس وبوب) على معلومات عامة معروفة لكليهما (Common Global Information) هي:

P : عدد أولي كبير (1024 bits على الأقل) g : مولد وهو جذر أولي لـ P حيث $P > g$

2. يختار بوب عدداً عشوائياً XB(خاص)بحيث : XB∈[1,P-1]

3. يولد بوب باستخدام قيمة XB قيمة عامة YB وفق العلاقة :

$$YB = g^{XB} mod\ P$$

4. يرسل بوب القيمة العامة YB إلى أليس

5. تختار أليس عدداً عشوائياً XA(خاص) بحيث: XA∈[1,P-1]

6. تولد أليس باستخدام قيمة XA قيمة عامة YA وفق العلاقة :

$$YA = g^{XA} mod\ P$$

7. ترسل أليس القيمة العامة YA إلى بوب

آلية عمل خوارزمية ديفي هيلمان لتبادل المفاتيح(2/3)

8. يولد بوب المفتاح السري (المتناظر) وفق العلاقة:

$$K = YA^{XB} mod\ P$$

9. تولد أليس المفتاح السري (المتناظر) وفق العلاقة:

$$K = YB^{XA} mod\ P$$

آلية عمل خوارزمية ديفي هيلمان لتبادل المفاتيح(3/3)

الاتفاق على قيم Pوg

ألیس

تختار عدداً عشوائياً XA

تولد قيمة عامة YA وفق العلاقة :

$$YA = g^{XA} mod\ P$$

ترسل YA

تولد المفتاح السري (المتناظر) وفق العلاقة:

$$K = YB^{XA} mod\ P$$

بوب

يختارعدداً عشوائياً XB

يولد قيمة عامة YB وفق العلاقة :

$$YB = g^{XB} mod\ P$$

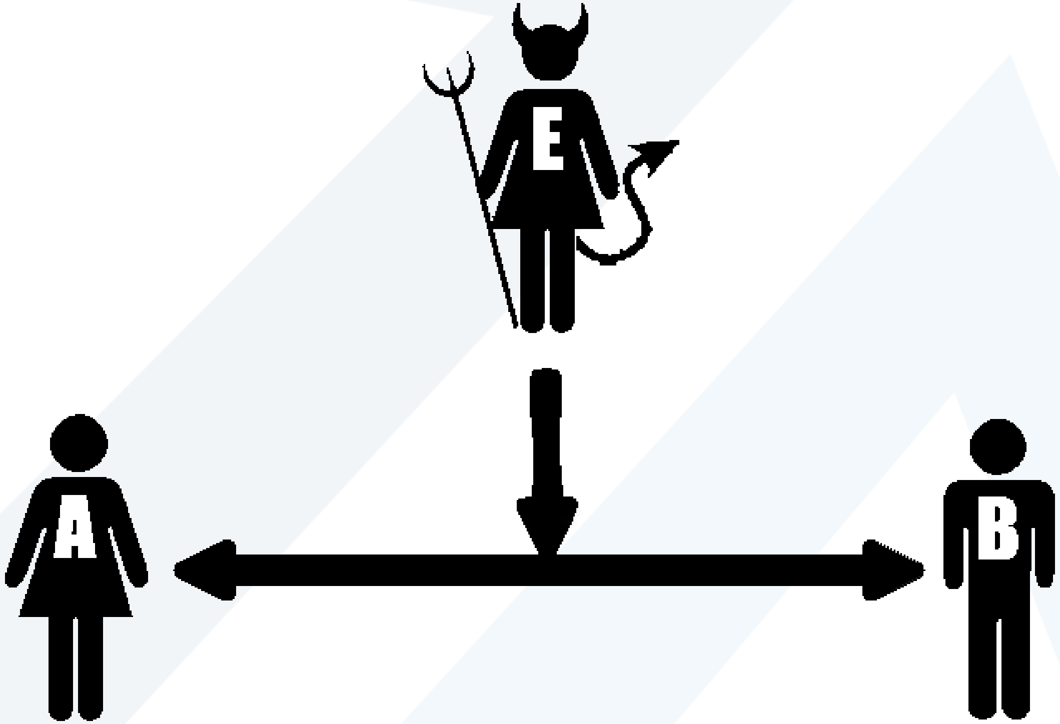
يرسل YB

يولد المفتاح السري (المتناظر) وفق العلاقة:

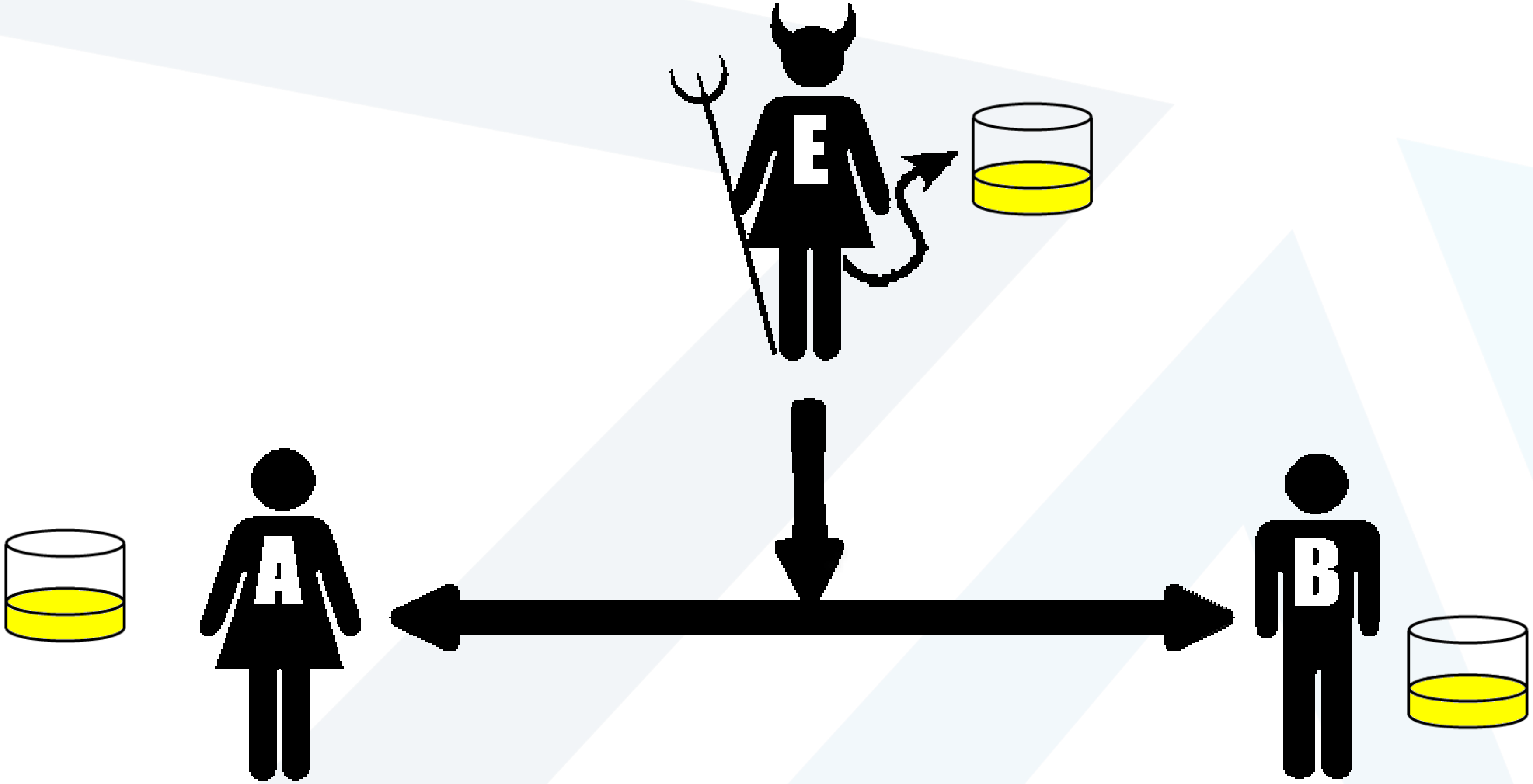
$$K = YA^{XB} mod\ P$$

أمن خوارزمية ديفي هيلمان لتبادل المفاتيح

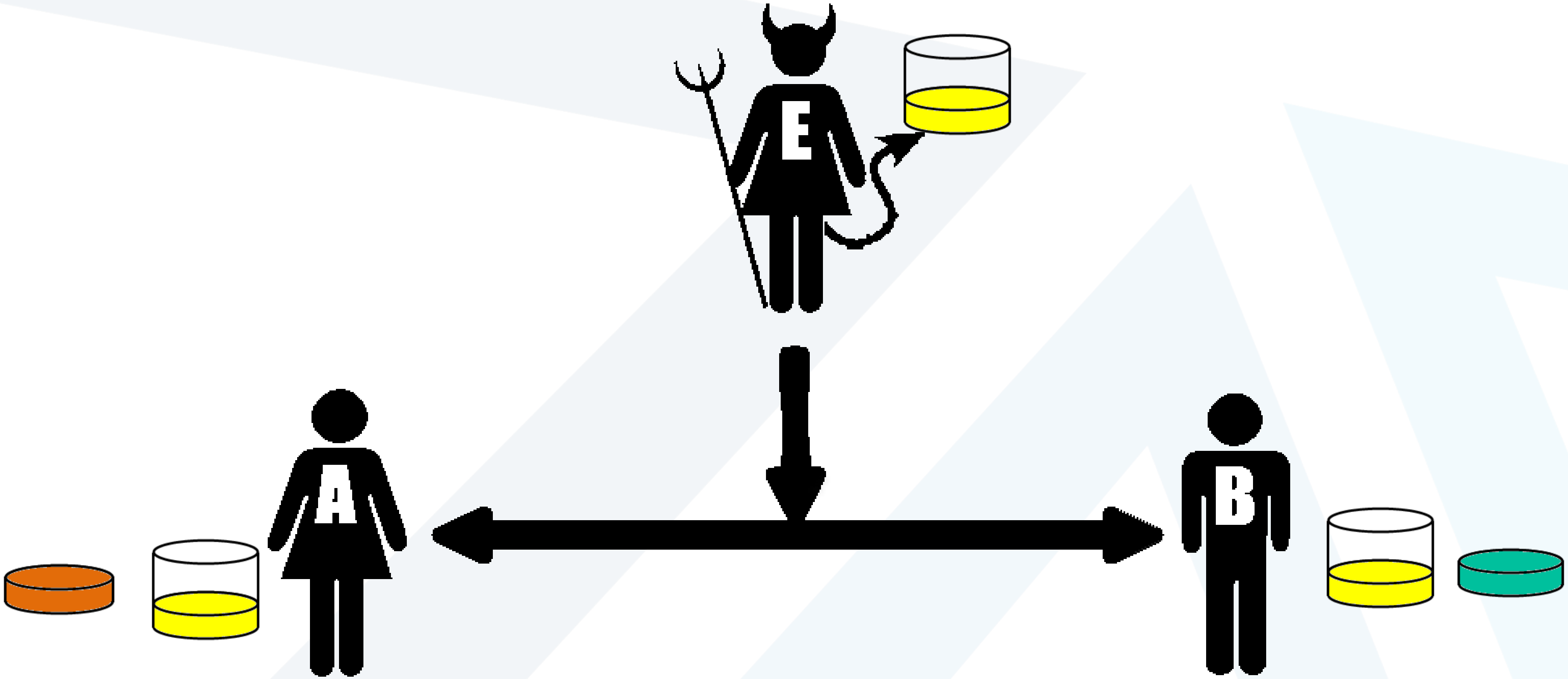
بفرض أن المهاجم ينصت لعمليات التبادل التي تجري بين أليس و بوب



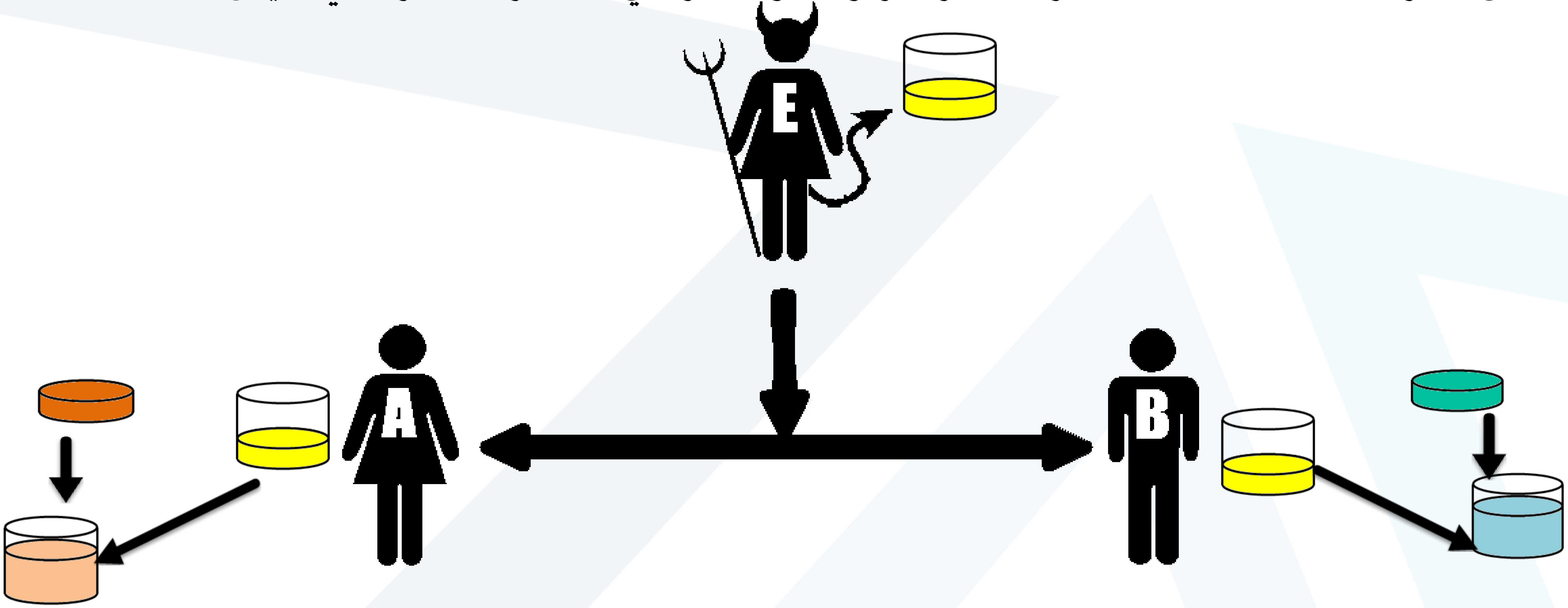
سيتفق كلاهما على القيم العامة المعروفة (اللون الأصفر)و كذلك سيحصل عليها المهاجم



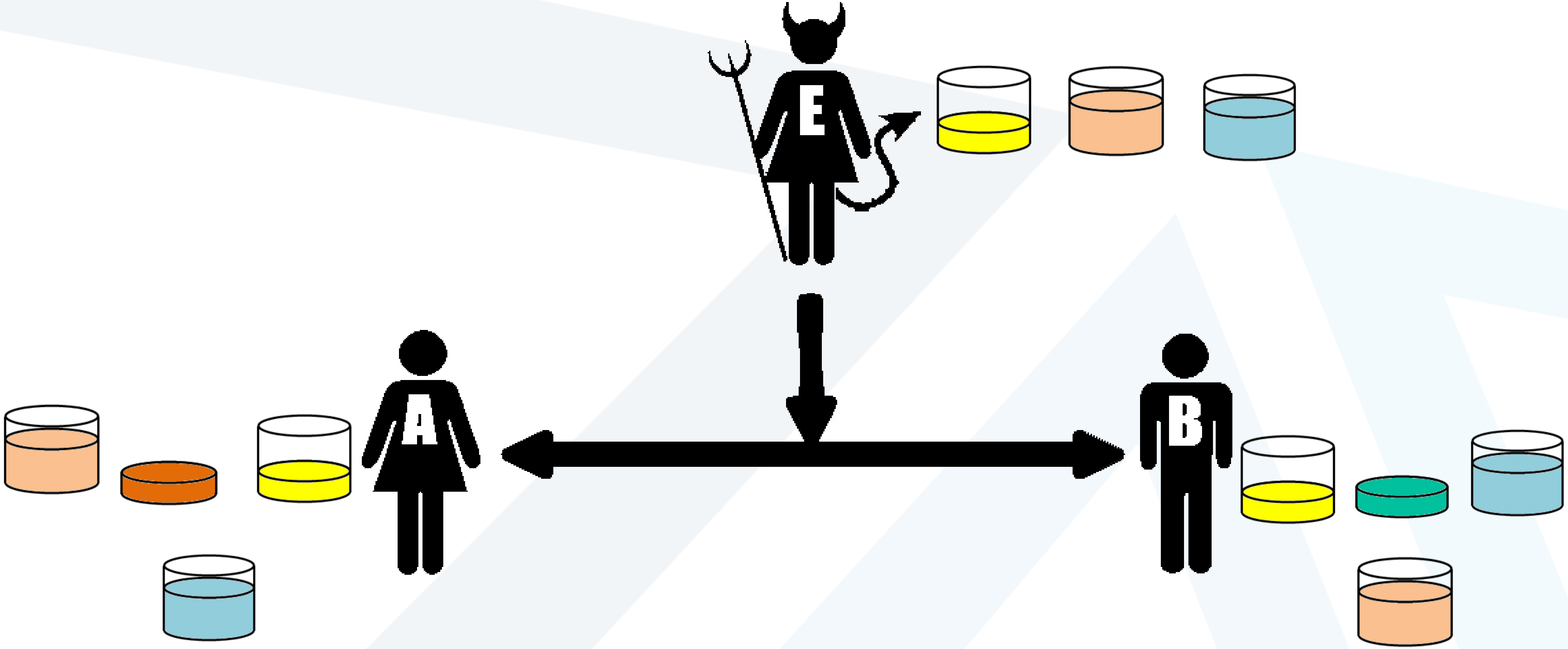
يختار كل من الطرفين قيمة سرية (اللون الأخضر لبوب، اللون البرتقالي لأليس)، لا يمكن للمهاجم معرفة أي منهما



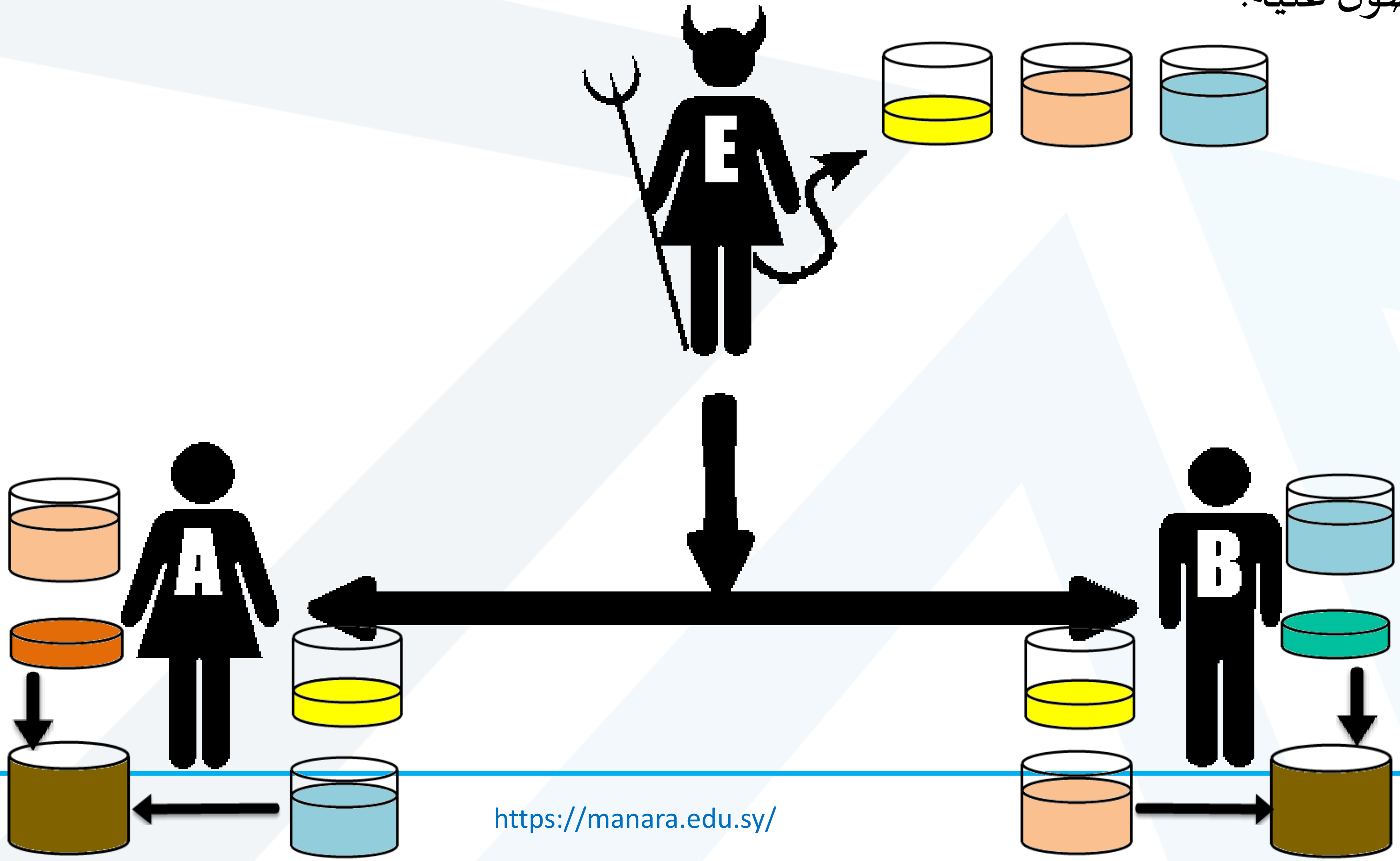
يولد كل من الطرفين قيمة علنية   (أخضر +أصفر =تركواز لبوب، برتقالي +أصفر =أصفر طيني لأليس)



يرسل كل من الطرفين القيمة العلنية للآخر (تركواز ،أصفر طيني) فيحصل عليها المهاجم



يولد كل من الطرفين المفتاح السري لهما بمفرده (أصفر طيني+ أخضر =عفني ، التركواز + برتقالي =عفني) لن يكون المهاجم قادراً على الحصول عليه.



أمن خوارزمية ديفي هيلمان رياضياً:

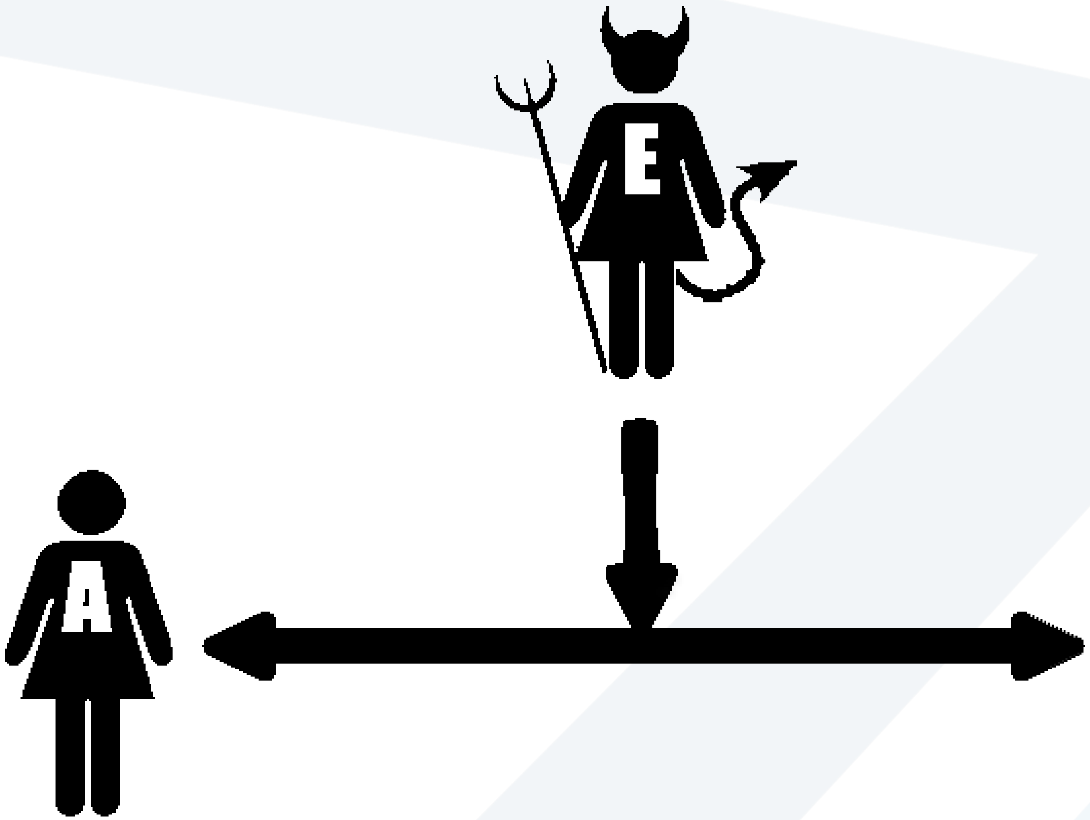
$$XA = \log_g(Y_A \bmod P)$$

$$XB = \log_g(Y_B \bmod P)$$

من الصعب جداً جداً الحصول على القيم السرية من القيم العلنية

لايمكن للمهاجم الحصول على المفتاح السري أو توليده

YA, YB, g ,P



YA
XA
g
p
YB

YB
XB
g
p
YA

نهاية المحاضرة الرابعة